Unit B2

Subgroups and isomorphisms

Introduction

In Unit B1 *Symmetry and groups* you met the idea of a group and studied a few basic properties of groups. In this unit you will be introduced to many of the fundamental ideas of group theory.

First you will meet the idea of a *subgroup* of a group. This is a group whose elements form a subset of the set of elements of another group, and whose binary operation is the same as for the other group. You will go on to look at what happens when a group element is repeatedly composed with itself, and see how this leads to a way of finding some of the subgroups of a group. You will also explore some properties of *cyclic groups*, which are groups in which every element can be obtained by repeatedly composing one particular element with itself. Finally, you will look at the idea that two groups may differ in their elements and binary operations, but have exactly the same underlying structure, so that, in an abstract sense, they are 'the same group'.

All the ideas covered in this unit help us gain insight into the structures of groups, enabling us to see and analyse some of the fundamental similarities and differences between various groups.

1 Subgroups

In this section you will see that groups can contain other groups.

1.1 What is a subgroup?

To illustrate the idea of a subgroup, let us consider the symmetry group of the equilateral triangle, $(S(\triangle), \circ)$, which you met in Unit B1. Recall that $S(\triangle) = \{e, a, b, r, s, t\}$, where the letters stand for the symmetries illustrated in Figure 1, and that $\circ$ represents function composition. The group table for $(S(\triangle), \circ)$ is as follows.

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

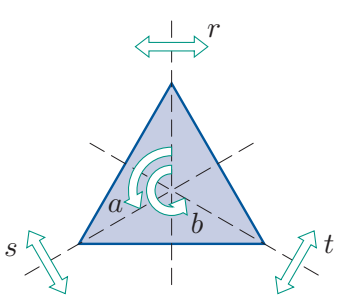


Figure 1 $S(\triangle)$

Now consider the set $\{e, a, b\}$ of *direct* symmetries of the equilateral triangle. We can obtain a Cayley table for this set under function composition by deleting the rows and columns labelled by the indirect symmetries in the group table of $(S(\triangle), \circ)$, as shown below.

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$(S(\triangle), \circ)$

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$(\{e, a, b\}, \circ)$

Let us check whether $(\{e, a, b\}, \circ)$ is a group. Here is a reminder of the group axioms.

Definition

Let G be a set and let $\circ$ be a binary operation defined on G. Then $(G, \circ)$ is a **group** if the following four axioms hold.

G1 Closure For all g, h in G,

$$g \circ h \in G.$$

G2 Associativity For all g, h, k in G,

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

G3 Identity There is an element e in G such that

$$g \circ e = g = e \circ g \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element** for $\circ$ on G.)

G4 Inverses For each element g in G, there is an element h in G such that

$$g \circ h = e = h \circ g.$$

(The element h is an **inverse element** of g with respect to $\circ$.)

We now check these axioms for $(\{e, a, b\}, \circ)$.

G1 Closure The only elements in the body of the Cayley table for $(\{e, a, b\}, \circ)$ are e, a and b, so $\{e, a, b\}$ is closed under function composition; that is, axiom G1 holds.

G2 Associativity We know that function composition is an associative binary operation, so axiom G2 holds.

G3 Identity The row and column labelled e in the Cayley table for $(\{e, a, b\}, \circ)$ repeat the table borders, so e is an identity element for $(\{e, a, b\}, \circ)$; that is, axiom G3 holds.

G4 Inverses We can see from the Cayley table for $(\{e, a, b\}, \circ)$ that each element of $\{e, a, b\}$ has an inverse element in $\{e, a, b\}$ (e is self-inverse and a and b are inverses of each other), so axiom G4 holds.

So all four group axioms hold, and hence $(\{e, a, b\}, \circ)$ is a group.

Since $\{e, a, b\}$ is a subset of $S(\triangle) = \{e, a, b, r, s, t\}$, and both these sets are groups under the same binary operation (namely function composition), we say that $(\{e, a, b\}, \circ)$ is a *subgroup* of $(S(\triangle), \circ)$. In general, we have the following definition.

Definition

A **subgroup** of a group $(G, \circ)$ is a group $(H, \circ)$, where H is a subset of G.

Notice that it is part of the definition of a subgroup that the subgroup has the *same* binary operation as the original group.

Now consider the subset $\{e, b\}$ of $S(\triangle)$. We can obtain a Cayley table for $(\{e, b\}, \circ)$ in the same way as we did for $(\{e, a, b\}, \circ)$. That is, we start with the group table of $(S(\triangle), \circ)$, and delete the rows and columns labelled by the elements of $S(\triangle)$ that are not elements of $\{e, b\}$, as follows.

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$(S(\triangle), \circ)$

$\longrightarrow$

$\circ$	e	b
e	e	b
b	b	a

$(\{e, b\}, \circ)$

The Cayley table for $(\{e, b\}, \circ)$ contains the element a, which is not in the set $\{e, b\}$. So $\{e, b\}$ is not closed under function composition; that is, axiom G1 fails. Thus $(\{e, b\}, \circ)$ is *not* a subgroup of $(S(\triangle), \circ)$.

Exercise B35

For each of the following, construct a Cayley table by deleting rows and columns of the group table for $(S(\triangle), \circ)$, and determine whether the given set and binary operation form a subgroup of $(S(\triangle), \circ)$.

(a) $(\{e, s\}, \circ)$ (b) $(\{e, b, r\}, \circ)$

Among the groups you met in Unit B1, some are subgroups of others. For example,

$(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$,

since $\mathbb{R} \subseteq \mathbb{C}$ and the binary operations of $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are the same. Similarly,

$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$, and

$(\mathbb{Q}^*, \times)$ is a subgroup of $(\mathbb{R}^*, \times)$.

In contrast,

$(\mathbb{R}^*, \times)$ is *not* a subgroup of $(\mathbb{R}, +)$.

This is because, although $\mathbb{R}^*$ is a subset of $\mathbb{R}$, the binary operations of the two groups are different.

In fact, every group $(G, \circ)$ with more than one element has at least two subgroups: the group $(G, \circ)$ itself, and the group $(\{e\}, \circ)$, known as the **trivial subgroup**, whose only element is the identity element. Some particular examples of the trivial subgroup of a group include:

the trivial subgroup $(\{e\}, \circ)$ of the group $(S(\triangle), \circ)$,

the trivial subgroup $(\{0\}, +)$ of the group $(\mathbb{Z}, +)$,

the trivial subgroup $(\{1\}, \times)$ of the group $(\mathbb{R}^*, \times)$.

A subgroup of a group $(G, \circ)$ other than the whole group $(G, \circ)$ is called a **proper subgroup**.

A subgroup $(H, \circ)$ of an abelian group $(G, \circ)$ is always abelian, because if $x \circ y = y \circ x$ for all elements x and y of G, then it must also be true that $x \circ y = y \circ x$ for all elements x and y of the subset H of G.

However, a non-abelian group can have an abelian subgroup. This is illustrated by the example at the start of this subsection: $(S(\triangle), \circ)$ is non-abelian but its subgroup $(\{e, a, b\}, \circ)$ is abelian, as you can see by looking at their group tables. (Recall that a finite group is abelian if and only if its group table is symmetric with respect to the main diagonal.)

Some texts use the notation $H \leq G$ to assert that H is a subgroup of G and the notation $H < G$ to assert that H is a proper subgroup of G, but we will not use these notations in M208.

Identities and inverses in subgroups

We now need to deal with two rather subtle issues that arise from the definition of a subgroup.

Consider a group $(G, \circ)$, with identity element e, and suppose that $(H, \circ)$ is a subgroup of $(G, \circ)$. Might the identity element of $(H, \circ)$ be an element other than e? In fact, this is *not* possible, as stated and proved below. The identity element of $(H, \circ)$ must be the same element as the identity element of $(G, \circ)$.

A similar issue arises with inverses of group elements. Again, consider a group $(G, \circ)$ and a subgroup $(H, \circ)$. Might there be an element h of H whose inverse in $(H, \circ)$ is a different element from its inverse in $(G, \circ)$? Again, this is *not* possible, as stated and proved below.

Theorem B23

Let $(G, \circ)$ be a group with a subgroup $(H, \circ)$.

(a) The identity element of $(H, \circ)$ is the same as the identity element of $(G, \circ)$.

(b) For each element h of H, the inverse of h in $(H, \circ)$ is the same as its inverse in $(G, \circ)$.

Proof

(a) Let the identity elements of $(G, \circ)$ and $(H, \circ)$ be e and e_H, respectively. Then $e_H \circ e_H = e_H$ (since e_H is the identity element of $(H, \circ)$), and $e \circ e_H = e_H$ (since e is the identity element of $(G, \circ)$, and $e_H \in G$). It follows that $e_H \circ e_H = e \circ e_H$, and hence, by the Right Cancellation Law, $e_H = e$.

(b) Let $h \in H$, and suppose that the inverse of h in H is a and the inverse of h in G is b. We know by part (a) that $(G, \circ)$ and $(H, \circ)$ have the same identity element, e say. Thus $h \circ a = e$ and $h \circ b = e$. It follows that $h \circ a = h \circ b$, and hence, by the Left Cancellation Law, $a = b$. ■

1.2 Checking whether a subset forms a subgroup

At the start of the previous subsection you saw that $(\{e, a, b\}, \circ)$ is a subgroup of $(S(\triangle), \circ)$. This was shown by checking each group axiom for $(\{e, a, b\}, \circ)$.

In fact, it was not necessary to carry out such extensive checks, because some properties hold for $(\{e, a, b\}, \circ)$ simply because they hold for $(S(\triangle), \circ)$. For example, we already know that $x \circ e = x = e \circ x$ for any element x of $S(\triangle)$, so the same must be true for any element x of the subset $\{e, a, b\}$ of $S(\triangle)$. So, to check that e is an identity element for $(\{e, a, b\}, \circ)$, all we really need to check is that e actually belongs to $\{e, a, b\}$. (Which of course it does!)

The next theorem sets out exactly what you need to check to show whether or not a subset of a group forms a subgroup.

Theorem B24 Subgroup test

Let $(G, \circ)$ be a group with identity element e, and let H be a subset of G. Then $(H, \circ)$ is a subgroup of $(G, \circ)$ if and only if the following three properties hold.

SG1 Closure For all x, y in H, the composite $x \circ y$ is in H.

SG2 Identity The identity element e of G is in H.

SG3 Inverses For each x in H, its inverse x^{-1} in G is in H.

We refer to the three properties SG1, SG2 and SG3 listed in the theorem as the three **subgroup properties**. Notice that although these properties have the same names as three of the group axioms, namely *Closure*, *Identity* and *Inverses*, only the closure property involves the same ideas as the corresponding group axiom. The other two properties involve only a check that certain elements (the identity element of G and the inverses of elements of H) *actually belong to* H: they do not involve a check that these elements have the defining properties of an identity element or inverse.

Proof of Theorem B24 First we prove the 'if' part. Suppose that the three subgroup properties hold. We need to check that $(H, \circ)$ is a group. To do that, we check that $(H, \circ)$ satisfies the four group axioms.

G1 Closure Property SG1 means the same as axiom G1, so axiom G1 holds.

G2 Associativity Since $(G, \circ)$ is a group, we know that

$$x \circ (y \circ z) = (x \circ y) \circ z$$

for all elements x, y, z in G, so this equation holds for all elements x, y, z in the subset H of G. Thus axiom G2 holds.

G3 Identity We have $e \in H$, since property SG2 holds, and if $x \in H$ then $x \circ e = x = e \circ x$, since $x \in G$ and e is the identity element of $(G, \circ)$. So e is an identity element for $\circ$ on H. Thus axiom G3 holds.

G4 Inverses Let $x \in H$. Then the inverse x^{-1} of x in G is also in H, since property SG3 holds, and we have $x \circ x^{-1} = e = x^{-1} \circ x$. So x^{-1} is an inverse of x in H. Thus axiom G4 holds.

Hence $(H, \circ)$ satisfies the four group axioms, and so is a group.

Now we prove the 'only if' part. Suppose that $(H, \circ)$ is a subgroup of $(G, \circ)$. We have to show that properties SG1, SG2 and SG3 hold. Since $(H, \circ)$ is a group, the set H is closed under $\circ$, so property SG1 holds. Also, by Theorem B23, H contains the identity element e of G and the inverse of each element of H, so properties SG2 and SG3 hold. ■

Theorem B24 tells us that if $(G, \circ)$ is a group and H is a subset of G, then to check that $(H, \circ)$ is a subgroup of $(G, \circ)$ we need only check that the three subgroup properties hold, rather than having to check the full group axioms. It also tells us that to show that $(H, \circ)$ is *not* a subgroup of $(G, \circ)$, we just need to show that *any one* of the three subgroup properties fails. (To do this, we give a counter-example, not a general argument.)

Remember that before you apply Theorem B24 you need to be sure that H is a subset of G, and that the binary operations on the two sets are the same. If these conditions do not hold, then $(H, \circ)$ is certainly not a subgroup of $(G, \circ)$.

The worked example below demonstrates how to use the three subgroup properties to determine whether or not $(H, \circ)$ is a subgroup of a group $(G, \circ)$, in cases where H is a small finite set. In this situation, particularly if you suspect that $(H, \circ)$ *is* a subgroup of $(G, \circ)$, it is often useful to start by constructing a Cayley table for $(H, \circ)$. You can then use the table to help you check the three subgroup properties. (In the worked example the group $(G, \circ)$ is finite, but the same approach can be used if $(G, \circ)$ is an infinite group.)

Worked Exercise B15

(a) Show that $(\{e, a, b, c\}, \circ)$ is a subgroup of $(S(\square), \circ)$.

(b) Show that $(\{e, r, s, t\}, \circ)$ is not a subgroup of $(S(\square), \circ)$.

(The non-identity elements of $S(\square)$ are shown in Figure 2.)

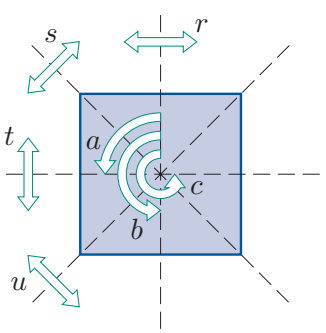


Figure 2 $S(\square)$

Solution

(a) We have $\{e, a, b, c\} \subseteq S(\square)$, and the binary operation $\circ$ is the same on each set.

Construct a Cayley table for $(\{e, a, b, c\}, \circ)$, by deleting the unwanted rows and columns of the group table of $(S(\square), \circ)$ (which is repeated as Table 1).

The Cayley table for $(\{e, a, b, c\}, \circ)$ is as follows.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

We check the three subgroup properties.

Use the Cayley table to check properties SG1 and SG3. To check for inverses, look for occurrences of the identity element in the table.

Table 1 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

SG1 Closure Every element in the body of the table is in $\{e, a, b, c\}$, so $\{e, a, b, c\}$ is closed under function composition.

SG2 Identity The identity element in $S(\square)$ is e, and $e \in \{e, a, b, c\}$.

SG3 Inverses The elements e and b are self-inverse, and a and c are inverses of each other, so $\{e, a, b, c\}$ contains the inverse of each of its elements.

Hence $(\{e, a, b, c\}, \circ)$ satisfies the three subgroup properties, and so is a subgroup of $(S(\square), \circ)$.

(b) We have $\{e, r, s, t\} \subseteq S(\square)$, and the binary operation $\circ$ is the same on each set.

However, $r, t \in \{e, r, s, t\}$ but $r \circ t = b \notin \{e, r, s, t\}$, so property SG1 fails.

Hence $(\{e, r, s, t\}, \circ)$ is not a subgroup of $(S(\square), \circ)$.

Exercise B36

Show that $(\{e, b, s, u\}, \circ)$ is a subgroup of $(S(\square), \circ)$.

Many of the exercises and worked exercises in the rest of this subsection involve subsets of the standard groups of numbers that you met in Unit B1. Here is a reminder of these groups.

Standard groups of numbers

Infinite groups

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +),$$
$$(\mathbb{Q}^*, \times), \quad (\mathbb{R}^*, \times), \quad (\mathbb{C}^*, \times).$$

Finite groups, for any integer $n \geq 2$:

$(\mathbb{Z}_n, +_n)$,

$(U_n, \times_n)$, and in particular $(\mathbb{Z}_p^*, \times_p)$, where p is prime.

Here $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ and $\mathbb{Z}_n^*$ mean $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_n$ with the element 0 removed, and U_n is the set of integers in $\mathbb{Z}_n$ coprime to n.

The next exercise involves a finite subgroup of one of the infinite groups above.

Exercise B37

(a) Construct a Cayley table for $(\{1, -1, i, -i\}, \times)$ (where $i^2 = -1$).

(b) Show that $(\{1, -1, i, -i\}, \times)$ is a subgroup of the group $(\mathbb{C}^*, \times)$.

So far, we have looked at how to check whether $(H, \circ)$ is a subgroup of a group $(G, \circ)$ only in the case where H is finite. If H is an *infinite* set, then we have to check the three subgroup properties by using algebraic arguments rather than a Cayley table. This is demonstrated in the next worked exercise.

Worked Exercise B16

Show that $(\mathbb{R}^+, \times)$ is a subgroup of the group $(\mathbb{R}^*, \times)$, where $\mathbb{R}^+$ denotes the set of positive real numbers.

Solution

We have $\mathbb{R}^+ \subseteq \mathbb{R}^*$, and the binary operation $\times$ is the same on each set.

We check the three subgroup properties.

SG1 Closure Let $x, y \in \mathbb{R}^+$; then $x, y \in \mathbb{R}$, $x > 0$ and $y > 0$. It follows that $x \times y \in \mathbb{R}$ and $x \times y > 0$, so $x \times y \in \mathbb{R}^+$. Thus $\mathbb{R}^+$ is closed under $\times$.

SG2 Identity The identity element in $(\mathbb{R}^*, \times)$ is 1. Since $1 > 0$, we have $1 \in \mathbb{R}^+$.

SG3 Inverses Let $x \in \mathbb{R}^+$. The inverse of x in $(\mathbb{R}^*, \times)$ is $1/x$. Since $x \in \mathbb{R}^+$, we have $x \in \mathbb{R}$ and $x > 0$. It follows that $1/x \in \mathbb{R}$ and $1/x > 0$, so $1/x \in \mathbb{R}^+$. Thus $\mathbb{R}^+$ contains the inverse of each of its elements.

Hence $(\mathbb{R}^+, \times)$ satisfies the three subgroup properties, and so is a subgroup of $(\mathbb{R}^*, \times)$.

The next exercise involves the set of integer multiples of 3; we denote this set by $3\mathbb{Z}$. That is,

$$3\mathbb{Z} = \{3k : k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}.$$

In general, for any number x, we denote the set of integer multiples of x by $x\mathbb{Z}$. That is,

$$x\mathbb{Z} = \{xk : k \in \mathbb{Z}\} = \{\ldots, -2x, -x, 0, x, 2x, 3x, \ldots\}.$$

Exercise B38

Show that $(3\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

The solution to Exercise B38 remains valid if the integer 3 is replaced by any integer n, so we have the following result.

For any integer n, $(n\mathbb{Z}, +)$ is a subgroup of the group $(\mathbb{Z}, +)$.

Exercise B39

(a) Is $(6\mathbb{Z}, +)$ a subgroup of $(\mathbb{Z}, +)$?

(b) Is $(6\mathbb{Z}, +)$ a subgroup of $(2\mathbb{Z}, +)$?

(c) Is $(5\mathbb{Z}, +)$ a subgroup of $(3\mathbb{Z}, +)$?

Justify your answers.

In the next worked exercise, Theorem B24 (Subgroup test) is used to show that a particular infinite subset is *not* a subgroup of a particular infinite group.

Worked Exercise B17

Show that $(\mathbb{Z}^+, +)$ is not a subgroup of the group $(\mathbb{Z}, +)$, where $\mathbb{Z}^+$ denotes the set of positive integers.

Solution

We have $\mathbb{Z}^+ \subseteq \mathbb{Z}$, and the binary operation $+$ is the same on each set.

However, the identity element in $(\mathbb{Z}, +)$ is 0, but $0 \notin \mathbb{Z}^+$, so property SG2 fails.

Hence $(\mathbb{Z}^+, +)$ is not a subgroup of $(\mathbb{Z}, +)$.

Exercise B40

(a) Show that $(\mathbb{Q}^*, \times)$ is not a subgroup of the group $(\mathbb{R}^+, \times)$.

(You saw that $(\mathbb{R}^+, \times)$ is a group in Worked Exercise B16.)

(b) Show that $(W, +)$ is not a subgroup of the group $(\mathbb{Z}, +)$, where W is the set of non-negative integers.

The following two exercises should familiarise you further with checking the subgroup properties.

Exercise B41

Show that $(H, +_{12})$ is a subgroup of the group $(\mathbb{Z}_{12}, +_{12})$, where $H = \{0, 3, 6, 9\}$.

Hint: In this case, it is easier to construct the Cayley table for $(H, +_{12})$ directly, rather than by deleting rows and columns from the group table for $(\mathbb{Z}_{12}, +_{12})$.

Exercise B42

In each of the following cases, H is a subset of G, but $(H, \circ)$ is not a subgroup of the group $(G, \circ)$. Explain why not.

(a) $(G, \circ) = (S(\square), \circ)$ and $(H, \circ) = (\{e, a, c\}, \circ)$.

(The non-identity elements of $S(\square)$ are shown in Figure 3.)

(b) $(G, \circ) = (\mathbb{Z}_5^*, \times_5)$ and $(H, \circ) = (\{2, 3, 4\}, \times_5)$.

(c) $(G, \circ) = (\mathbb{R}^*, \times)$ and $(H, \circ) = (\mathbb{Z}^*, \times)$.

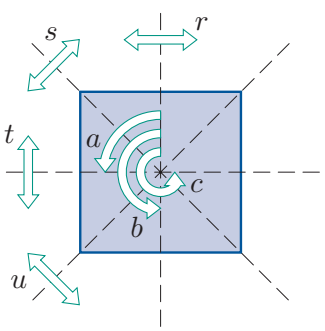


Figure 3 $S(\square)$

An unfamiliar binary operation

The final worked exercise and exercise in this subsection involve subsets of a group with an unfamiliar binary operation. They give you an opportunity to revise checking all the group axioms, as well as to practise checking the three subgroup properties.

Worked Exercise B18

Let X be the subset of $\mathbb{R}^2$ consisting of all the points not on the y-axis; that is,

$$X = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}.$$

Let $*$ be the binary operation on X defined by

$$(a, b) * (c, d) = (ac, ad + b).$$

For example, $(2, 5) * (4, 3) = (2 \times 4, 2 \times 3 + 5) = (8, 11)$.

(a) Show that $(X, *)$ is a group.

(b) Determine whether each of the following subsets of X together with the binary operation $*$ forms a subgroup of $(X, *)$.

(i) $A = \{(a, b) \in X : a = 1\}$

(ii) $B = \{(a, b) \in X : b = 1\}$

Solution

(a) We check the four group axioms.

G1 Closure

If we combine two elements of X using $*$, do we get another element of X? To check this, start with two general elements of X and combine them.

Let $(a, b), (c, d) \in X$; then $a, b, c, d \in \mathbb{R}$, and $a \neq 0$ and $c \neq 0$. We have

$$(a, b) * (c, d) = (ac, ad + b).$$

To check that this point is in X, we have to check that it is in $\mathbb{R}^2$ and its first coordinate is non-zero.

Now $(ac, ad + b) \in \mathbb{R}^2$ because $a, b, c, d \in \mathbb{R}$, and $ac \neq 0$ because $a \neq 0$ and $c \neq 0$, so $(ac, ad + b) \in X$. Thus X is closed under $*$.

G2 Associativity

Since $*$ is an unfamiliar binary operation, we must use an algebraic argument to prove associativity.

Let $(a, b), (c, d), (e, f) \in X$. We have

$$\begin{aligned}(a, b) * ((c, d) * (e, f)) &= (a, b) * (ce, cf + d)\\ &= (ace, acf + ad + b)\end{aligned}$$

and

$$\begin{aligned}((a, b) * (c, d)) * (e, f) &= (ac, ad + b) * (e, f)\\ &= (ace, acf + ad + b).\end{aligned}$$

The two expressions obtained are the same, so $*$ is associative on X.

G3 Identity

Try to find a likely candidate to be an identity.

Suppose that (e, f) is an identity in X. Then we must have, for each $(a, b) \in X$,

$$(a, b) * (e, f) = (a, b) = (e, f) * (a, b).$$

The left-hand equation gives

$$(ae, af + b) = (a, b).$$

Comparing coordinates gives

$$ae = a \quad \text{and} \quad af + b = b;$$

that is,

$$ae = a \quad \text{and} \quad af = 0.$$

Since these equations must hold for all non-zero values of a, we must have $e = 1$ and $f = 0$. So the only possibility for an identity is $(1, 0)$.

Now check to see whether this point actually is an identity.

Now $(1,0) \in X$, since it is in $\mathbb{R}^2$ and its first coordinate is non-zero, and for all $(a,b) \in X$, we have

$$(a,b) * (1,0) = (a \times 1, a \times 0 + b) = (a,b)$$

and

$$(1,0) * (a,b) = (1 \times a, 1 \times b + 0) = (a,b).$$

So $(1,0)$ is an identity for $*$ on X.

G4 Inverses

Try to find a likely candidate to be an inverse of a general element $(a,b) \in X$.

Let $(a,b) \in X$; then $a \neq 0$. Suppose that (c,d) is an inverse of (a,b). Then we must have

$$(a,b) * (c,d) = (1,0) = (c,d) * (a,b).$$

The left-hand equation gives

$$(ac, ad + b) = (1,0).$$

Comparing coordinates gives

$$ac = 1 \quad \text{and} \quad ad + b = 0.$$

Try to find c and d in terms of a and b.

Since $a \neq 0$, these equations give

$$c = \frac{1}{a} \quad \text{and} \quad d = -\frac{b}{a}.$$

So the only possibility for an inverse of (a,b) is $(1/a, -b/a)$.

Now check to see whether this point actually is an inverse of (a,b).

Now $(1/a, -b/a) \in X$, since it is in $\mathbb{R}^2$ (because a and b are in $\mathbb{R}$ and a is non-zero) and its first coordinate is non-zero, and we have

$$(a,b) * \left(\frac{1}{a}, -\frac{b}{a}\right) = \left(a \times \frac{1}{a},\ a \times \left(-\frac{b}{a}\right) + b\right) = (1,0)$$

and

$$\left(\frac{1}{a}, -\frac{b}{a}\right) * (a,b) = \left(\frac{1}{a} \times a,\ \frac{1}{a} \times b - \frac{b}{a}\right) = (1,0).$$

So $(1/a, -b/a)$ is an inverse of (a,b). Thus every element of X has an inverse in X.

Hence $(X, *)$ satisfies the four group axioms, and so is a group.

(b) (i) Simplify the description of A, if possible, to make it easier to work with.

We have

$$A = \{(a, b) \in X : a = 1\} = \{(1, b) : b \in \mathbb{R}\}.$$

We check the three subgroup properties for A.

SG1 Closure

Start with two general elements of A, combine them using $*$, and check that the result is in A.

Let $(1, b), (1, d) \in A$. We have

$$(1, b) * (1, d) = (1 \times 1, 1 \times d + b) = (1, d + b).$$

This point is in A because its first coordinate is 1. Thus A is closed under $*$.

SG2 Identity

The identity element in $(X, *)$ is $(1, 0)$. This point has first coordinate 1, so it is in A.

SG3 Inverses

Let $(1, b) \in A$. By the solution to part (a), the inverse of $(1, b)$ in $(X, *)$ is

$$\left(\frac{1}{1}, -\frac{b}{1}\right) = (1, -b).$$

This point has first coordinate 1, so it is in A. Thus A contains the inverse of each of its elements.

Hence $(A, *)$ satisfies the three subgroup properties, and so is a subgroup of $(X, *)$.

(ii) Simplify the description of B, if possible, to make it easier to work with.

We have

$$B = \{(a, b) \in X : b = 1\} = \{(a, 1) : a \in \mathbb{R}, a \neq 0\}.$$

We can see immediately that the identity $(1, 0)$ of $(X, *)$ is not in B, so there is no need to check the other subgroup properties.

The identity in $(X, *)$ is $(1, 0)$, but this point is not in B, so property SG2 fails.

Hence $(B, *)$ is not a subgroup of $(X, *)$.

The group $(X, *)$ defined in Worked Exercise B18 is non-abelian, as you can check by working out $(1, 1) * (2, 2)$ and $(2, 2) * (1, 1)$ for example. In contrast, the different group $(X, *)$ defined in the next exercise is abelian, because for this group $(a, b) * (c, d) = (c, d) * (a, b)$ for all $(a, b), (c, d) \in X$.

Exercise B43

Let X be the set

$$X = \{(a, b) \in \mathbb{R}^2 : a, b \neq 0\}$$

and let $*$ be the binary operation on X defined by

$$(a, b) * (c, d) = (ac, bd).$$

(a) Show that $(X, *)$ is a group.

(b) Determine whether each of the following subsets of X together with the binary operation $*$ forms a subgroup of $(X, *)$.

(i) $A = \{(a, b) \in X : a = 1\}$

(ii) $B = \{(a, b) \in X : a + b = 2\}$

When we are discussing groups, and subgroups of groups, it can be cumbersome to keep using notation of the form $(G, \circ)$, in which both the set of the group and the binary operation are included. For this reason, from now on we will often use the following convention.

Convention

We can refer to a group $(G, \circ)$ simply as G, as long as the binary operation is clear from the context.

So we might say, for example:

- 'the subgroup H of the group G'
- 'the symmetry group $S(F)$ of the figure F'
- 'the set H is a subgroup of the group G'
- 'the set $\{e, a, b, c\}$ is a subgroup of the group G'.

When you see phrases like these, or when you use them yourself, you should keep in mind that a group is definitely *not just a set*, but consists of both a set and a binary operation. When you are reading about a group or working with a group it is important that you know what the binary operation is.

Because of the convention above, if $(G, \circ)$ is a group then an instance of the notation G could mean either the group $(G, \circ)$ or simply the set G. Often it does not matter which meaning applies; for example, this is the case for the statement 'Let g be an element of G.' If it does matter, then the meaning should be clear from the context.

1.3 Subgroups of symmetry groups

In Unit B1 you saw that the symmetries of any figure F in $\mathbb{R}^2$ or $\mathbb{R}^3$ form a group under function composition called the **symmetry group** of F and denoted by $S(F)$. In this subsection we will look at some ways in which we can find subgroups of the symmetry group of a figure.

The subgroup of direct symmetries of a figure

First, as stated in the theorem below, the set $S^+(F)$ of *direct* symmetries of a figure F always forms a subgroup of its symmetry group $S(F)$. Of course, if the figure F has no indirect symmetries, then $S^+(F)$ and $S(F)$ are the same set.

Theorem B25

Let F be a figure in $\mathbb{R}^2$ or $\mathbb{R}^3$. Then the set $S^+(F)$ of direct symmetries of F is a subgroup of the symmetry group $S(F)$ of F.

Proof We have $S^+(F) \subseteq S(F)$, and the binary operation $\circ$ is the same on each set. We check the three subgroup properties, using the properties of direct and indirect symmetries given in Subsection 1.4 of Unit B1.

SG1 Closure Composing any two direct symmetries gives a direct symmetry, so $S^+(F)$ is closed under $\circ$.

SG2 Identity The identity element e of $S(F)$ is a direct symmetry, so it is in $S^+(F)$.

SG3 Inverses If f is a direct symmetry, then f^{-1} is also a direct symmetry. So $S^+(F)$ contains the inverse of each of its elements.

Hence $S^+(F)$ satisfies the three subgroup properties, and so is a subgroup of $S(F)$. ■

For example, the set $S^+ = \{e, a, b\}$ of direct symmetries of the equilateral triangle is a subgroup of the symmetry group $S(\triangle)$ of the equilateral triangle, as you saw at the start of this unit.

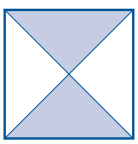
Modifying a figure

Another way in which we can sometimes find subgroups of a symmetry group $S(F)$ is to modify the figure F to restrict its symmetry. We could, for example, modify a square F by introducing a pattern of shapes, as illustrated in Worked Exercise B19 below. The modified square F' is still a plane figure (a subset of $\mathbb{R}^2$): it consists of all the points that lie on the lines or in the shaded areas. The symmetry group $S(F')$ of the modified square consists of those symmetries of the square that leave the pattern of shapes unchanged.

Worked Exercise B19

Let F' be the modified square shown below. Write down a subgroup of $S(\square)$ by listing the symmetries of the figure F'.

(For convenience, Figure 4 shows the non-identity elements of $S(\square)$.)



F'

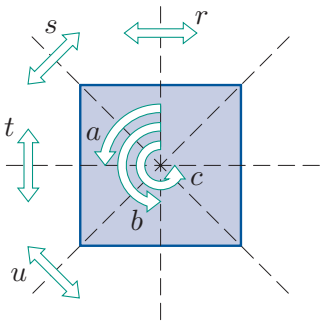


Figure 4 $S(\square)$

Solution

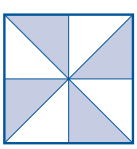
The effect of the modification is that the rotations a and c and the reflections s and u, which are symmetries of the unmodified square, are no longer symmetries of the figure.

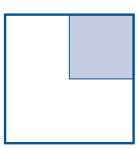
A subgroup of $S(\square)$ is

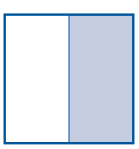
$$S(F') = \{e, b, r, t\}.$$

Exercise B44

Write down three subgroups of $S(\square)$ by listing the elements of the symmetry groups of each of the following modified squares.

(a) 

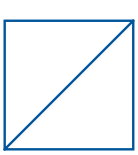
(b) 

(c) 

We often use a simple pattern of line segments to restrict the symmetries of a figure. In the following worked exercise, a single diagonal line is used to restrict the symmetries of a square. Again, the modified square F' is still a plane figure: in this case it consists of all the points that lie on the lines.

Worked Exercise B20

Write down a subgroup of $S(\square)$ by listing the symmetries of the following modified square F'.



Solution

The effect of adding the diagonal line is that the rotations a and c and the reflections r and t, which are symmetries of the unmodified square, are no longer symmetries of the figure.

A subgroup of $S(\square)$ is

$$S(F') = \{e, b, s, u\}.$$

Exercise B45

Let F be a regular hexagon. Describe geometrically the elements of the subgroup $S(F')$ of $S(F)$, where F' is the figure obtained by inscribing an equilateral triangle inside F as shown.

Fixing a feature of a figure

A third possible way to find a subgroup of a symmetry group $S(F)$ is to fix some feature of the figure, such as a vertex or an edge. That is, we consider only the elements of $S(F)$ that map that feature to itself. For example, consider the square with its usual vertex location labels, as shown in Figure 5. If we fix the vertex at location 1, that is, if we consider only the symmetries that map this vertex to itself, then we obtain the subset $\{e, s\}$ of $S(\square)$. Fixing a subset of a figure always yields a subgroup of the symmetry group of the figure, as stated in the theorem below.

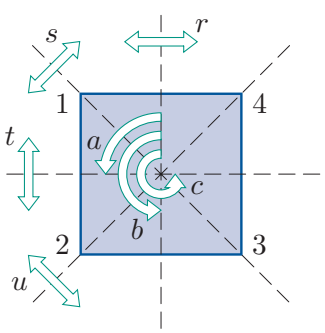


Figure 5 The square with its usual location labels

The feature of a figure that we fix can consist of any subset of the points that make up the figure. If the subset consists of more than one point, then the subset can be fixed without every individual point in the subset being fixed. For example, for the square in Figure 5, if we fix the edge that joins the vertices at locations 1 and 4, then we obtain the subset $\{e, r\}$ of $S(\square)$. The symmetry r fixes the edge described, even though it does not fix each point on this edge.

Theorem B26

Let F be a figure in $\mathbb{R}^2$ or $\mathbb{R}^3$ and let A be a subset of F. Then the subset of $S(F)$ whose elements are all the symmetries of F that fix A is a subgroup of $S(F)$.

Proof Let H be the subset of $S(F)$ described. We show that the three subgroup properties hold for H.

SG1 Closure Let f and g be symmetries of F that fix A. Then $g \circ f$ also fixes A. Hence H is closed under function composition.

SG2 Identity The identity symmetry fixes A, so H contains the identity element of $S(F)$.

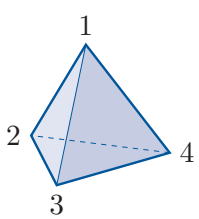
SG3 Inverses Let f be a symmetry of F that fixes A. Then f^{-1} also fixes A. Thus H contains the inverse of each of its elements.

Hence H satisfies the three subgroup properties, and so is a subgroup of $S(F)$. ■

We now use the method of fixing vertices to find some subgroups of the symmetry group of a regular tetrahedron, which we will denote by $S(\text{tet})$. You met the symmetries of the regular tetrahedron in Subsection 5.3 of Unit B1, and you may find it helpful to refresh your memory of these before continuing. As in Unit B1, we specify a symmetry in $S(\text{tet})$ by using a two-line symbol that indicates how the vertex at each location is affected by the symmetry.

Worked Exercise B21

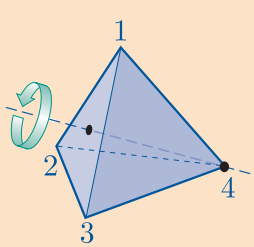
Consider the labelled regular tetrahedron shown below.



Write down, as two-line symbols, the elements of the subgroup of $S(\text{tet})$ that consists of the symmetries of the tetrahedron that fix the vertex at location 4.

Solution

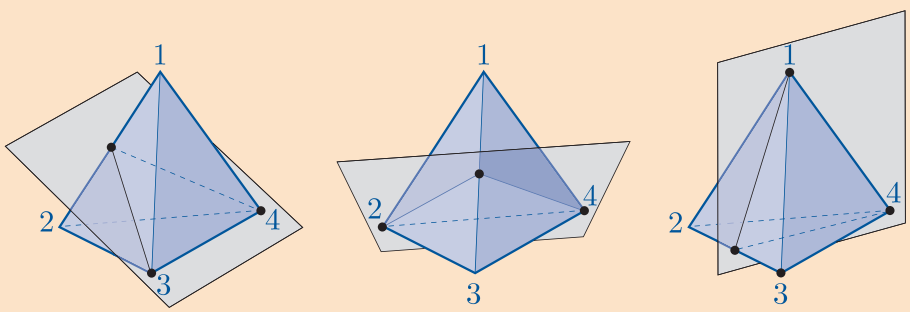
The direct symmetries of the tetrahedron that fix the vertex at location 4 are the three rotations through 0, $2\pi/3$ and $4\pi/3$ radians about the line through this vertex and the centre of the opposite face.



These are the symmetries

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}.$$

The indirect symmetries that fix the vertex at location 4 are reflections in three planes. Each such plane contains one of the three edges that meet at the vertex at location 4, and passes through the midpoint of the opposite edge.



These are the symmetries

$$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}.$$

The required subgroup is

$$\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\right\}.$$

Notice that the elements of the subgroup in Worked Exercise B21 look exactly like the elements of $S(\triangle)$, the symmetry group of an equilateral triangle, written as two-line symbols, but with an extra column, mapping 4 to 4, at the end. This is because each symmetry of the tetrahedron that fixes the vertex at location 4 gives a symmetry of the face with vertices at locations 1, 2 and 3.

In a similar way, we can find subgroups of $S(\text{tet})$ that fix the vertices at locations 1, 2 and 3, respectively. The elements of the subgroup that fixes the vertex at location 1 look like the elements of $S(\triangle)$ written as two-line symbols, but with the vertices of the triangle labelled 2, 3 and 4, and with an extra column mapping 1 to 1. Similar descriptions apply to the other two subgroups.

Exercise B46

Write down, as two-line symbols, the elements of the subgroup of $S(\text{tet})$ that consists of the symmetries of the tetrahedron shown in Worked Exercise B21 that fix the vertex at location 3.

Exercise B47

Write down, as two-line symbols, the elements of the subgroup of $S(\text{tet})$ that consists of the symmetries of the tetrahedron shown in Worked Exercise B21 that fix the edge joining the vertices at locations 1 and 2.

The strategy below summarises the methods that you have seen for finding subgroups of the symmetry group of a figure.

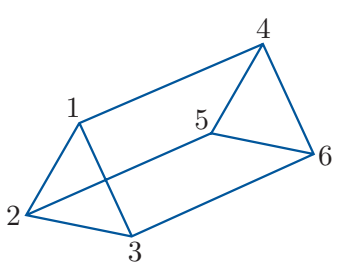
Strategy B3

To find a subgroup of the symmetry group of a figure in $\mathbb{R}^2$ or $\mathbb{R}^3$, do *one* of the following.

- Find the direct symmetries of the figure.
- Modify the figure to restrict its symmetry; for example, introduce a pattern of lines or shapes. Then determine which of the symmetries of the original figure are symmetries of the new figure.
- Find the symmetries of the figure that fix a particular vertex (or any other particular subset of the figure).

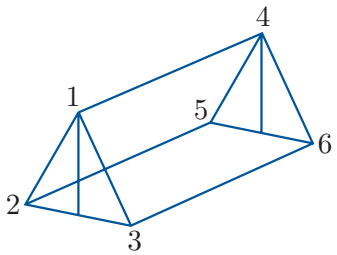
Exercise B48

Let F be the wire framework of a triangular prism, labelled as shown below. The triangles at its ends are equilateral, and its other faces are rectangles.

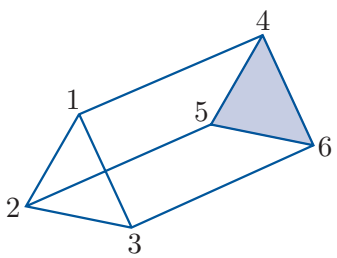


Find three subgroups of $S(F)$ by considering the following ways of restricting the symmetry. Give each symmetry as a two-line symbol.

(a) Add a vertical wire to each of the triangular ends of the framework prism, as shown below.



(b) Fill in a triangular face at one end of the framework prism, as shown below.



(c) Fix the vertices at locations 1 and 4.

2 Order of a group element

In this section we will explore what happens when we take an element of a group and repeatedly combine it with itself.

2.1 Powers of a group element

Before we can proceed, we need a notation for writing down repeated combinations of an element. We normally use index notation. If $(G, \circ)$ is a group, and x is an element of G, then we write

x^2 to represent $x \circ x$,
x^3 to represent $x \circ x \circ x$,
x^4 to represent $x \circ x \circ x \circ x$,

and so on. We interpret x^1 to mean just x itself, and x^0 to mean e, the identity element of G.

We also attach a meaning to negative powers of a group element. You have seen that x^{-1} represents the inverse of x. We also write

x^{-2} to represent $x^{-1} \circ x^{-1}$,
x^{-3} to represent $x^{-1} \circ x^{-1} \circ x^{-1}$,
x^{-4} to represent $x^{-1} \circ x^{-1} \circ x^{-1} \circ x^{-1}$,

and so on.

Here is a summary of this notation.

Powers of a group element

Powers of an element x of a group $(G, \circ)$ are defined as follows. Let n be a positive integer. Then

$$x^0 = e, \quad \text{the identity element}$$

$$x^n = \underbrace{x \circ x \circ \cdots \circ x}_{n \text{ copies of } x}$$

$$x^{-n} = \underbrace{x^{-1} \circ x^{-1} \circ \cdots \circ x^{-1}}_{n \text{ copies of } x^{-1}}.$$

Each power of x is an element of G, since G is closed under $\circ$.

Worked Exercise B22

Find the following powers in the group $S(\square)$:

$$c^0,\ c^1,\ c^2,\ c^3,\ c^4,\ c^5.$$

(The non-identity elements of $S(\square)$ are shown in Figure 6.)

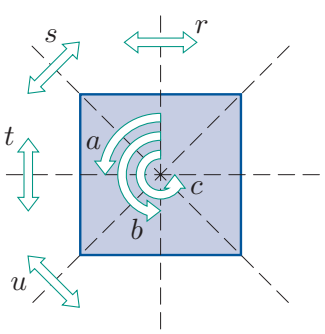


Figure 6 $S(\square)$

Solution

$c^0 = e,$

$c^1 = c,$

$c^2 = c \circ c$
$= b,$

$c^3 = c \circ c \circ c$
$= c^2 \circ c$
$= b \circ c$
$= a,$

$c^4 = c \circ c \circ c \circ c$
$= c^3 \circ c$
$= a \circ c$
$= e,$

$c^5 = c \circ c \circ c \circ c \circ c$
$= c^4 \circ c$
$= e \circ c$
$= c.$

Exercise B49

Find the following powers in the group $S(\square)$.

(a) $a^0, a^1, a^2, a^3, a^4, a^5$

(b) $a^{-1}, a^{-2}, a^{-3}, a^{-4}, a^{-5}$

(c) b^0, b^1, b^2, b^3, b^4

(d) b^{-1}, b^{-2}, b^{-3}

(e) r^0, r^1, r^2, r^3, r^4

The following familiar index laws hold for the powers of a group element.

Theorem B27 Index laws

Let x be an element of a group $(G, \circ)$, and let m and n be integers. The following index laws hold.

(a) $x^m \circ x^n = x^{m+n}$

(b) $(x^m)^n = x^{mn}$

(c) $(x^n)^{-1} = x^{-n} = (x^{-1})^n$

Proof Proofs of the laws in the case where m and n are positive integers are given or commented on below. The other cases, where m and n might be zero or negative, can be proved in similar ways, using the definitions of x^0 and negative powers of x. The details are omitted here.

Let x be an element of a group $(G, \circ)$, and let m and n be positive integers.

(a) We have

$$\begin{aligned} x^m \circ x^n &= \underbrace{x \circ x \circ \cdots \circ x}_{m \text{ copies of } x} \circ \underbrace{x \circ x \circ \cdots \circ x}_{n \text{ copies of } x} \\ &= \underbrace{x \circ x \circ \cdots \circ x}_{m+n \text{ copies of } x} \\ &= x^{m+n}. \end{aligned}$$

(b) We have

$$\begin{aligned} (x^m)^n &= \underbrace{x^m \circ x^m \circ \cdots \circ x^m}_{n \text{ copies of } x^m} \\ &= \underbrace{\underbrace{x \circ x \circ \cdots \circ x}_{m \text{ copies of } x} \circ \underbrace{x \circ x \circ \cdots \circ x}_{m \text{ copies of } x} \circ \cdots \circ \underbrace{x \circ x \circ \cdots \circ x}_{m \text{ copies of } x}}_{n \text{ 'blocks'}} \\ &= \underbrace{x \circ x \circ \cdots \circ x}_{mn \text{ copies of } x} \\ &= x^{mn}. \end{aligned}$$

(c) The fact that $x^{-n} = (x^{-1})^n$, where n is a positive integer, is simply the definition of a negative power of a group element. You are asked to prove that $(x^n)^{-1} = (x^{-1})^n$ in the case $n = 2$ in the exercise below, and a proof for any positive integer n follows in a similar way. ■

Exercise B50

Let x be an element of a group $(G, \circ)$. Show that the inverse of x^2 is $(x^{-1})^2$.

Using index notation to denote repeated combinations of group elements works well for any group in which the binary operation is some kind of multiplication, and for any group in which the binary operation is function composition, such as a group of symmetries.

However, it is not appropriate for groups in which the binary operation is some kind of addition. For example, it would be confusing to denote the composite $x + x + x$ in the group $(\mathbb{R}, +)$ by x^3. Instead, we denote it by $3x$, in the familiar way, and we refer to it as a **multiple** rather than a power.

So there are two types of notation that we can use for combinations of elements in groups: **multiplicative notation** and **additive notation**. These two types of notation also include different ways of representing other features of groups, such as the identity element and inverse elements. A summary is given in the box below.

Multiplicative notation and additive notation for groups

Feature	Multiplicative notation	Additive notation
Composite	$a \circ b$ or $a \times b$ or ab (or similar)	$a + b$ (or similar)
Identity	e or 1	0
Inverse	x^{-1}	$-x$
Power/multiple	x^n	nx

We always use multiplicative notation for groups in which the binary operation is some kind of multiplication, or function composition. We also use it for abstract groups, in which the binary operation is not specified as being of any particular type. A group for which we use multiplicative notation is called a **multiplicative** group.

We use additive notation for groups in which the binary operation is some kind of addition, such as addition of numbers, or modular addition. A group for which we use additive notation is called an **additive** group. Additive groups are always abelian, because addition is a commutative operation.

It is important to remember that a multiple in an additive group means the same as a power in a multiplicative group. For example, if x is an element of a multiplicative group $(G, \circ)$, then

$$x \circ x \circ x \circ x = x^4,$$

and if x is an element of an additive group $(G, +)$, then

$$x + x + x + x = 4x.$$

Similarly, if x is an element of a multiplicative group $(G, \circ)$, then

$$x^{-1} \circ x^{-1} \circ x^{-1} = (x^{-1})^3 = x^{-3},$$

and if x is an element of an additive group $(G, +)$, then

$$(-x) + (-x) + (-x) = 3(-x) = -3x.$$

Theorems, proofs and general discussions about group theory are normally expressed in multiplicative notation, both in this module and in mathematics in general. If you want to apply them to additive groups, then you have to translate them into additive notation. For example, here is Theorem B27 translated into additive notation. These laws should look familiar to you in this form too.

Theorem B28 Index laws (in additive notation)

Let x be an element of a group $(G, +)$, and let m and n be integers. The following laws hold.

(a) $mx + nx = (m + n)x$

(b) $n(mx) = (nm)x$

(c) $-(nx) = (-n)x = n(-x)$

Exercise B51

Translate the following statements about elements x and y of a multiplicative group $(G, \circ)$ into additive notation for elements x and y of an additive group $(G, +)$.

(a) $x^0 = e$ (b) $x \circ x^{-1} = e$ (c) $x \circ x^2 = x^3$ (d) $(x^{-1})^{-1} = x$

(e) $e \circ x = x$ (f) $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$

2.2 What is the order of a group element?

Now that we have the notation we need, let us look at what happens when we take an element of a group and repeatedly combine it with itself. In Exercise B49 you should have found that when you take the element a of the group $S(\square)$ and find the powers a, a^2, a^3, a^4 and so on, eventually you reach a power that is equal to the identity element e of the group. You should have found the same for the elements b and r of $S(\square)$. To enable us to describe situations like these, we make the definitions in the box below. Note that the word *order* in these definitions has a different meaning from the word *order* used to mean the size of a group. However, the two uses of the word are connected, as you will see in Section 3.

Definitions

Let x be an element of a group $(G, \circ)$.

If there is a positive integer n such that $x^n = e$, then the **order** of x is the *smallest* positive integer n such that $x^n = e$. We say that x has **finite order**.

If there is no positive integer n such that $x^n = e$, then x has **infinite order**.

For example, consider the following list of all the powers of the element a of the group $S(\square)$; the list includes the negative powers, and the zeroth power, as well as the positive powers. The powers are evaluated in the second line below (using Figure 7).

$$\ldots,\ a^{-4},\ a^{-3},\ a^{-2},\ a^{-1},\ a^0,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7,\ a^8,\ a^9,\ \ldots$$
$$\ldots,\ e,\quad a,\quad b,\quad c,\quad e,\quad a,\ b,\ c,\ e,\ a,\ b,\ c,\ e,\ a,\ \ldots$$

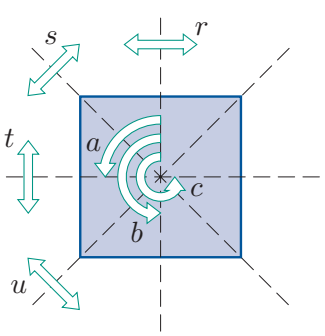


Figure 7 $S(\square)$

The list shows that, for example, $a^{-4} = e$, $a^0 = e$, $a^4 = e$, and $a^8 = e$. The *smallest positive* integer n such that $a^n = e$ is 4, so a has order 4.

Similarly, consider the powers of 2 in the group $(\mathbb{R}^*, \times)$:

$$\ldots,\ 2^{-3},\ 2^{-2},\ 2^{-1},\ 2^0,\ 2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7,\ \ldots$$
$$\ldots,\ \tfrac{1}{8},\quad \tfrac{1}{4},\quad \tfrac{1}{2},\quad 1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 128,\ \ldots$$

The identity element of $(\mathbb{R}^*, \times)$ is 1, and there is no *positive* integer n such that $2^n = 1$, so 2 has infinite order in $(\mathbb{R}^*, \times)$.

Finally, consider the multiples of 2 in the additive group $(\mathbb{R}, +)$:

$$\ldots,\ (-3)\times 2,\ (-2)\times 2,\ (-1)\times 2,\ 0\times 2,\ 2,\ 2\times 2,\ 3\times 2,\ \ldots$$
$$\ldots,\ -6,\ -4,\ -2,\ 0,\ 2,\ 4,\ 6,\ \ldots$$

The identity element of $(\mathbb{R}, +)$ is 0, and there is no *positive* integer n such that $n \times 2 = 0$, so 2 has infinite order in $(\mathbb{R}, +)$.

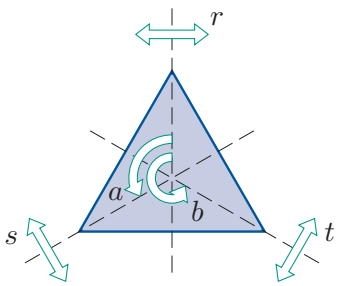


Figure 8 $S(\triangle)$

Worked Exercise B23

Find the order of the element a of $S(\triangle)$.

(The non-identity elements of $S(\triangle)$ are shown in Figure 8.)

Solution

We have

$$a^2 = a \circ a = b,$$
$$a^3 = a^2 \circ a = b \circ a = e.$$

Thus a in $S(\triangle)$ has order 3.

Alternatively, the smallest (positive) number of times that we need to apply a to bring the triangle back to its starting position is 3, so a has order 3.

Exercise B52

Find the orders of the following group elements.

(a) The element c in $S(\square)$. (b) The element r in $S(\square)$.

(c) The element 1 in $(\mathbb{Z}_6, +_6)$. (d) The element 2 in $(\mathbb{Z}_6, +_6)$.

(e) The element 5 in $(U_9, \times_9)$. (f) The element 9 in $(U_{10}, \times_{10})$.

(g) The element 1 in $(\mathbb{Z}, +)$. (h) The element i in $(\mathbb{C}^*, \times)$.

Exercise B53

State the order of each element in the group $(\mathbb{Z}, +)$.

An element of a finite group always has finite order, as shown next.

Theorem B29

Let x be an element of a finite group $(G, \circ)$. Then x has finite order.

Proof Consider the list of consecutive powers of x:

$$\ldots, x^{-4}, x^{-3}, x^{-2}, x^{-1}, x^0, x, x^2, x^3, x^4, \ldots.$$

The elements in this list cannot all be distinct, because they are all in G and there are only finitely many elements in G. So there must be integers s and t, with $s < t$, such that

$$x^s = x^t.$$

Composing each side of this equation with $(x^s)^{-1}$ on the right gives

$$x^s \circ (x^s)^{-1} = x^t \circ (x^s)^{-1}.$$

Simplifying (using the index laws on the right-hand side) gives

$$e = x^{t-s}.$$

Now $t - s$ is positive, since $s < t$. So there is a positive power of x that is equal to e, and hence x has finite order. ■

An element of an *infinite* group can have either finite order or infinite order. For example, in Exercise B52(h) you saw that the element i of the infinite group $(\mathbb{C}^*, \times)$ has finite order, and you saw earlier that the element 2 of the infinite group $(\mathbb{R}^*, \times)$ has infinite order.

The box below gives two simple results about the orders of group elements that are useful to remember.

Order of the identity and order of self-inverse elements

Let $(G, \circ)$ be a group with identity element e.

- The identity element e has order 1.
- If the element x is self-inverse, and $x \neq e$, then x has order 2.

The first result holds because $e^1 = e$, so the smallest positive integer n such that $e^n = e$ is 1. The second result holds because if $x = x^{-1}$ then (by composing each side by x) we have $x^2 = e$. This tells us that, provided $x \neq e$, the smallest positive integer n such that $x^n = e$ is 2.

Here is another useful result about the orders of group elements.

Theorem B30

If x is an element of a group $(G, \circ)$, then either x and x^{-1} have the *same* finite order, or they both have infinite order.

Proof Let $x \in G$ and let the identity element of $(G, \circ)$ be e.

First we show that for any integer n,

$$x^n = e \quad \text{if and only if} \quad (x^{-1})^n = e. \tag{1}$$

To do this, let $n \in \mathbb{Z}$ and first suppose that

$$x^n = e.$$

Composing each side on the right by $(x^n)^{-1}$ gives

$$x^n \circ (x^n)^{-1} = e \circ (x^n)^{-1}.$$

Simplifying, and using the index laws on the right-hand side, gives

$$e = (x^{-1})^n.$$

So we have shown that

$$\text{if } x^n = e, \text{ then } (x^{-1})^n = e.$$

Since this statement holds if we replace x by any element of G, it holds if we replace x by x^{-1}. So, since $(x^{-1})^{-1} = x$, we have that

$$\text{if } (x^{-1})^n = e, \text{ then } x^n = e.$$

Thus statement (1) holds. This statement tells us that the values of n for which $x^n = e$ are exactly the same as the values of n for which $(x^{-1})^n = e$. It follows that either x and x^{-1} have the same finite order, or they both have infinite order. ■

Now that you have met the idea of the order of a group element, let us go back to looking at what happens when we repeatedly combine a group element with itself. Look again at the list of consecutive powers of the element a in the group $S(\square)$:

$$\begin{array}{l} \ldots,\ a^{-4},\ a^{-3},\ a^{-2},\ a^{-1},\ a^0,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7,\ a^8,\ a^9,\ \ldots \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad \| \\ \ldots,\ e,\quad a,\quad b,\quad c,\quad e,\ a,\ b,\ c,\ e,\ a,\ b,\ c,\ e,\ a,\ \ldots \end{array}$$

The element a has order 4, and it looks as if a pattern of 4 distinct elements, namely e, a, b, c, keeps repeating indefinitely in the list of the powers of a.

In contrast, the element 2 in the group $(\mathbb{R}^*, \times)$ has infinite order, and all the elements in its list of powers are *distinct*:

$$\begin{array}{l} \ldots,\ 2^{-3},\ 2^{-2},\ 2^{-1},\ a^0,\ 2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7,\ \ldots \\ \qquad\qquad\qquad\quad \| \\ \ldots,\ \tfrac{1}{8},\ \tfrac{1}{4},\ \tfrac{1}{2},\ 1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 128,\ \ldots \end{array}$$

In general, we have the following important result.

Theorem B31

Let x be an element of a group $(G, \circ)$.

(a) If x has finite order n, then the n powers

$$e,\ x,\ x^2,\ \ldots,\ x^{n-1}$$

are distinct, and these elements repeat indefinitely every n powers in the list of consecutive powers of x.

(b) If x has infinite order, then all the powers of x are distinct.

Proof

(a) Suppose that x has finite order n.

First, we prove by contradiction that the n powers

$$e,\ x,\ x^2,\ \ldots,\ x^{n-1}$$

are distinct. Suppose that these powers are *not* distinct. Then

$$x^s = x^t$$

for some s and t with $0 \leq s < t \leq n-1$. Composing each side of this equation on the right with $(x^s)^{-1}$, and arguing as in the proof of Theorem B29, we can deduce that

$$e = x^{t-s}.$$

But $0 < t - s < n$ (since $0 \leq s < t \leq n-1$), so this contradicts the fact that n is the *smallest* positive integer such that $x^n = e$. It follows that the n powers listed above are all distinct.

Now we prove that the powers repeat every n elements. Consider any power of x of the form x^{kn}, where $k \in \mathbb{Z}$; that is, any power where the exponent is an integer multiple of the order n of x. We have

$$x^{kn} = (x^n)^k = e^k = e.$$

So, in the list of consecutive powers of x, the element e is repeated every n elements. Because each element in the list is obtained from the previous element by composing it with x, it follows that all the elements in the list repeat every n elements.

(b) You are asked to prove this part in the next exercise. ■

Exercise B54

Use a contradiction argument to prove Theorem B31(b).

2.3 Finding the orders of group elements

When you want to find the orders of all the elements in some finite group, you can cut down your work by using some of the results that you met in the previous subsection: the identity element has order 1, all other self-inverse elements have order 2, and an element and its inverse always have the same order. This is illustrated in the worked exercise below.

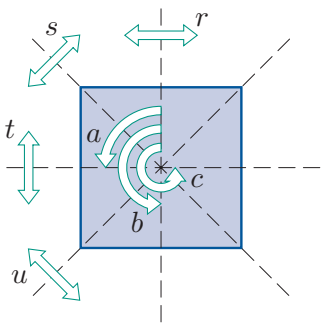


Figure 9 $S(\square)$

Worked Exercise B24

Find the order of every element in each of the following groups.

(a) $S(\square)$ (b) $(\mathbb{Z}_6, +_6)$

(See Figure 9 for a summary of the non-identity elements of $S(\square)$.)

Solution

(a) The identity element e has order 1.

The working needed to find the order of the element a of $S(\square)$ was part of what you were asked to do in Exercise B49.

For the element a, we have

$$a^2 = a \circ a = b,$$
$$a^3 = a^2 \circ a = b \circ a = c,$$
$$a^4 = a^3 \circ a = c \circ a = e.$$

Thus a has order 4. Hence c, the inverse of a, also has order 4.

All the other elements of $S(\square)$ are self-inverse and hence have order 2.

In summary, the orders of the elements of $S(\square)$ are as follows.

Element	e	a	b	c	r	s	t	u
Order	1	4	2	4	2	2	2	2

(b) The identity element 0 has order 1.

You found the orders of the elements 1 and 2 of $(\mathbb{Z}_6, +_6)$ in Exercise B52.

For the element 1, we have

$$1 +_6 1 = 2$$
$$1 +_6 1 +_6 1 = 3$$
$$1 +_6 1 +_6 1 +_6 1 = 4$$
$$1 +_6 1 +_6 1 +_6 1 +_6 1 = 5$$
$$1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0$$

Thus 1 has order 6. Hence 5, the inverse of 1, also has order 6.

For the element 2, we have

$$2 +_6 2 = 4$$
$$2 +_6 2 +_6 2 = 0$$

Thus 2 has order 3. Hence 4, the inverse of 2, also has order 3.

Finally, the element 3 is self-inverse, so it has order 2.

In summary, the orders of the elements of $(\mathbb{Z}_6, +_6)$ are as follows.

Element	0	1	2	3	4	5
Order	1	6	3	2	3	6

Exercise B55

Find the order of every element in each of the following groups.

(a) $S(\triangle)$ (b) $S(\square)$ (c) $(\mathbb{Z}_5^*, \times_5)$ (d) $(\mathbb{Z}_8, +_8)$

(The non-identity elements of $S(\triangle)$ and $S(\square)$ are shown in Figures 10 and 11.)

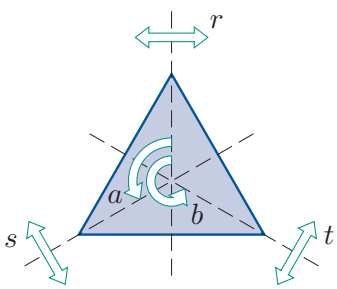


Figure 10 $S(\triangle)$

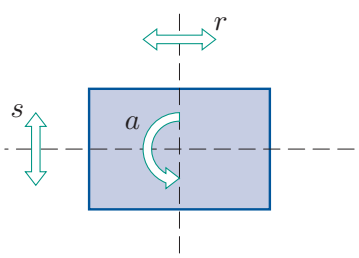


Figure 11 $S(\square)$

It is useful to think of the powers of a group element of finite order as forming a cycle. Theorem B31(a) tells us that, if we take a group element x of finite order n, and find its powers x^2, x^3, and so on, then successive powers cycle indefinitely through n distinct group elements, as illustrated in Figure 12. Once we reach x^{n-1}, the next element is e, and then the cycle repeats.

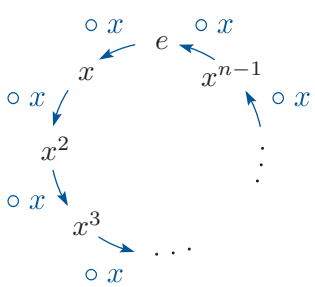


Figure 12 The effect of repeatedly composing a group element x of order n with itself

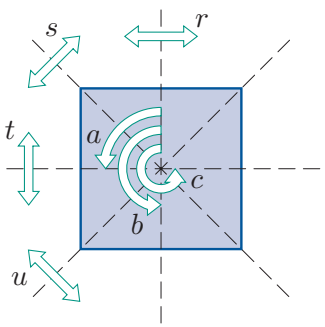


Figure 14 $S(\square)$

For example, Figure 13(a) shows what happens when we find powers of the element a in $S(\square)$, and Figure 13(b) shows what happens when we find multiples of the element 1 in $(\mathbb{Z}_6, +_6)$. (The non-identity elements of $S(\square)$ are shown again in Figure 14.)

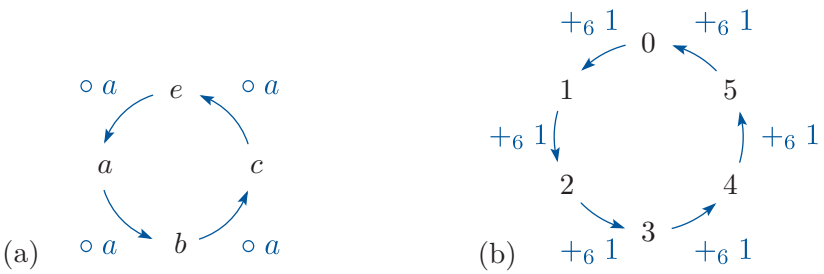


Figure 13 (a) The cycle of powers of the element a in $S(\square)$ (b) the cycle of multiples of the element 1 in $(\mathbb{Z}_6, +_6)$

You can use cycles like those in Figure 13 to find the powers of any of the group elements that appear in the cycle, and this can help you cut down your work further when you want to find the orders of group elements.

For example, consider the cycle of powers of the element a of $S(\square)$ in Figure 13(a). Moving one place round the cycle corresponds to composing by a. So moving one place round the cycle *in the reverse direction*, as shown by the inner arrows in Figure 15(a), corresponds to composing by a^{-1}, that is, composing by c. So if we start from e and go round the cycle in the reverse direction, then we will obtain the powers $e, c, c^2, c^3, c^4, \ldots$. Hence this list of powers evaluates to $e, c, b, a, e, \ldots$. This shows in particular that c has order 4, as found in Worked Exercise B24, which is as expected, since a group element and its inverse have the same order.

Similarly, moving *two* places round this cycle *in the original direction*, as shown by the inner arrows in Figure 15(b), corresponds to composing by a^2, that is, composing by b. So if we start from e and go round the cycle two places at a time in the direction of the arrows, then we will obtain the powers $e, b, b^2, b^3, b^4, \ldots$. Hence this list of powers evaluates to $e, b, e, b, e, \ldots$, which shows that b has order 2, as also found in Worked Exercise B24.

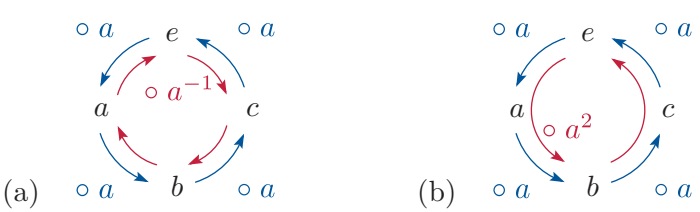


Figure 15 Moving round the cycle of powers of a in $S(\square)$ (a) in the reverse direction (b) in the original direction, two places at a time

Notice that the element that appears immediately before the identity element e in the cycle of powers of a in $S(\square)$ (shown in Figure 13(a)) is c, the inverse of a. This is because multiplying this element by a gives e. In general, we have the following fact.

Let x be a group element of finite order. In the cycle of powers of x, the element that appears immediately before the identity element is the inverse of x.

Exercise B56

(a) Write down the elements of the group $(U_{20}, \times_{20})$, and use any method to find the order of every element of this group.

(b) Use any method to find the order of every element of the group $(\mathbb{Z}_{12}, +_{12})$.

3 Cyclic subgroups and cyclic groups

The ideas that you met in the previous section give us a way of finding some of the subgroups of a group, and can also give us an insight into the structure of some groups, as you will see in this section.

3.1 The subgroup generated by an element

In this subsection we consider the set formed by all the powers of a group element.

Definition

Let x be an element of a group $(G, \circ)$. The set of all powers of x is called the subset of G **generated** by x, and denoted by $\langle x \rangle$. That is,

$$\langle x \rangle = \{x^k : k \in \mathbb{Z}\}.$$

In additive notation, if x is an element of a group $(G, +)$, then the subset of G generated by x is the set of all multiples of x:

$$\langle x \rangle = \{kx : k \in \mathbb{Z}\}.$$

A subset of a group generated by an element may be either finite or infinite, as illustrated by the worked exercise below.

Worked Exercise B25

Find the following generated subsets.

(a) The subset $\langle a \rangle$ of the group $S(\square)$.

(b) The subset $\langle 2 \rangle$ of the group $(\mathbb{R}, \times)$.

(c) The subset $\langle 2 \rangle$ of the group $(\mathbb{Z}_6, +_6)$.

Solution

(a) We saw earlier (near the start of Subsection 2.2) that the list of consecutive powers of a in $S(\square)$ is

$$\ldots, e, a, b, c, e, a, b, c, e, a, b, c, \ldots.$$

Hence

$$\langle a \rangle = \{e, a, b, c\}.$$

(b) In $(\mathbb{R}, \times)$, we have

$$\begin{aligned}\langle 2 \rangle &= \{2^k : k \in \mathbb{Z}\} \\ &= \{\ldots, 2^{-4}, 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, 2^4, \ldots\} \\ &= \{\ldots, \tfrac{1}{16}, \tfrac{1}{8}, \tfrac{1}{4}, \tfrac{1}{2}, 1, 2, 4, 8, 16, \ldots\}.\end{aligned}$$

(c) In $(\mathbb{Z}_6, +_6)$, the list of consecutive multiples of 2 is

$$\ldots, 0, 2, 4, 0, 2, 4, 0, 2, 4, \ldots.$$

Hence

$$\langle 2 \rangle = \{0, 2, 4\}.$$

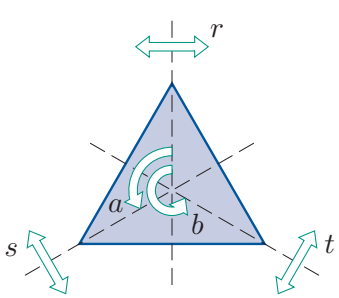


Figure 16 $S(\triangle)$

Exercise B57

Find the following generated subsets.

(a) The subset $\langle a \rangle$ of the group $S(\triangle)$.

(b) The subset $\langle 3 \rangle$ of the group $(\mathbb{Z}_7^*, \times_7)$.

(c) The subset $\langle 2 \rangle$ of the group $(\mathbb{Z}, +)$.

A reminder of the non-identity elements of $S(\triangle)$ is given in Figure 16.

The generated subsets found in Worked Exercise B25 and Exercise B57 are in fact all *subgroups* of the groups mentioned. This follows from the following theorem, which applies to both finite and infinite groups.

Theorem B32

Let x be an element of a group $(G, \circ)$. Then $(\langle x \rangle, \circ)$ is a subgroup of $(G, \circ)$.

Proof We check that the three subgroup properties hold.

SG1 Closure Let g and h be elements of $\langle x \rangle$. Then $g = x^s$ and $h = x^t$ for some integers s and t. So

$$g \circ h = x^s \circ x^t = x^{s+t}.$$

Thus $g \circ h$ can be written as a power of x, so $g \circ h \in \langle x \rangle$.

SG2 Identity The identity element e of $(G, \circ)$ can be written as $e = x^0$, so it is in $\langle x \rangle$.

SG3 Inverses Let g be any element of $\langle x \rangle$. Then $g = x^s$ for some integer s. Now

$$\begin{aligned} g^{-1} &= (x^s)^{-1} \\ &= x^{-s} \quad \text{(by one of the index laws).} \end{aligned}$$

Thus g^{-1} can be written as a power of x, so $g^{-1} \in \langle x \rangle$.

Since all three subgroup properties hold, $(\langle x \rangle, \circ)$ is a subgroup of $(G, \circ)$. ■

If x is an element of a group $(G, \circ)$, then we usually denote the subgroup $(\langle x \rangle, \circ)$ of G simply by $\langle x \rangle$, because the binary operation is clear from the context. We call this subgroup the **cyclic subgroup** of G **generated** by x. We also say that x is a **generator** of $\langle x \rangle$.

The order of the subgroup $\langle x \rangle$ (that is, the number of elements that it contains) is determined by the order of the element x, as set out in the next theorem. This theorem provides a connection between the two uses of the word 'order' in group theory, namely for the order of a group element (the smallest positive power or multiple of the element that equals the identity) and for the order of a group (the number of elements in the group).

Theorem B33

Let x be an element of a group.

(a) If x has finite order n, then the subgroup $\langle x \rangle$ has order n.

In multiplicative notation,

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}.$$

In additive notation,

$$\langle x \rangle = \{0, x, 2x, \ldots, (n-1)x\}.$$

(b) If x has infinite order, then the subgroup $\langle x \rangle$ has infinite order.

In multiplicative notation,

$$\langle x \rangle = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}.$$

In additive notation,

$$\langle x \rangle = \{\ldots, -2x, -x, 0, x, 2x, \ldots\}.$$

Proof This theorem follows immediately from Theorem B31. ■

As an illustration of Theorem B33, consider the element a of $S(\square)$. It has order 4, and the cyclic subgroup $\langle a \rangle = \{e, a, b, c\}$ that it generates has order 4 (that is, it has 4 elements). As another illustration, consider the element 2 of $(\mathbb{Z}, +)$. It has infinite order, and it generates a cyclic subgroup of infinite order, as you saw in Exercise B57(c).

Note that the subgroup of $(\mathbb{Z}, +)$ generated by 2 is the subgroup $(2\mathbb{Z}, +)$:

$$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} = 2\mathbb{Z}.$$

In general, for any integer n, the subgroup of $(\mathbb{Z}, +)$ generated by n is the subgroup $(n\mathbb{Z}, +)$.

The following results about cyclic subgroups follow from the simple results about the order of a group element that you met in Subsection 2.2 (Theorem B30 and the preceding box).

Some special cyclic subgroups

Let $(G, \circ)$ be a group with identity element e, and let $x \in G$.

- $\langle e \rangle = \{e\}$.
- If x is self-inverse and $x \neq e$, then $\langle x \rangle = \{e, x\}$.
- $\langle x^{-1} \rangle = \langle x \rangle$.

Proof The first two results here follow from the properties in the box that precedes Theorem B30. For the third result, x^{-1} is an element of the subgroup generated by x, so $\langle x^{-1} \rangle$ is a subgroup of $\langle x \rangle$. Also, $x = (x^{-1})^{-1}$

is an element of the subgroup generated by x^{-1}, so $\langle x \rangle$ is a subgroup of $\langle x^{-1} \rangle$. It follows that $\langle x^{-1} \rangle$ and $\langle x \rangle$ are equal. ■

When you want to find the cyclic subgroup generated by each element in some group, the working that you need to carry out is essentially the same as the working you need to carry out to find the orders of all the elements in the group. This is illustrated in the next worked exercise. You can cut down the work needed by using the results in the box above, and by using the techniques that you met in Subsection 2.3.

Worked Exercise B26

Find the cyclic subgroup generated by each element in the following groups.

(a) $S(\square)$ (see Figure 17) (b) $(\mathbb{Z}_6, +_6)$

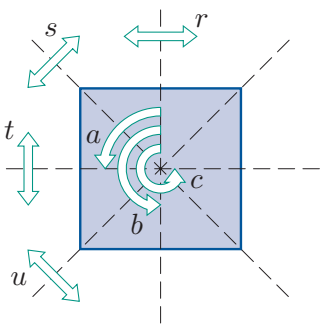


Figure 17 $S(\square)$

Solution

(a) Since e is the identity element in $S(\square)$, we have

$$\langle e \rangle = \{e\}.$$

To find the cyclic subgroup $\langle a \rangle$, find the consecutive powers of a, starting at the identity element e and stopping when e is reached again.

The powers of a are

$$a^0 = e, \quad a^1 = a, \quad a^2 = b, \quad a^3 = c, \quad a^4 = e, \quad \ldots.$$

So

$$\langle a \rangle = \{e, a, b, c\}.$$

Use the fact that an element and its inverse generate the same cyclic subgroup.

The element c is the inverse of a, so

$$\langle c \rangle = \{e, a, b, c\}.$$

The remaining elements are all self-inverse, so

$$\langle b \rangle = \{e, b\},$$
$$\langle r \rangle = \{e, r\},$$
$$\langle s \rangle = \{e, s\},$$
$$\langle t \rangle = \{e, t\},$$
$$\langle u \rangle = \{e, u\}.$$

As you would expect from Theorem B33, the orders of the cyclic subgroups of $S(\square)$ agree with the orders of their generators, which we found in Worked Exercise B24.

(b) Since 0 is the identity element in $(\mathbb{Z}_6, +_6)$, we have

$$\langle 0 \rangle = \{0\}.$$

To find the cyclic subgroup $\langle 1 \rangle$, find the consecutive multiples of 1, starting at the identity element 0 and stopping when 0 is reached again. Of course, finding consecutive multiples of 1 is trivial!

The multiples of 1 in $(\mathbb{Z}_6, +_6)$ are

$$\ldots, 0, 1, 2, 3, 4, 5, 0, \ldots,$$

and 5 is the inverse of 1, so

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\},$$
$$\langle 5 \rangle = \{0, 1, 2, 3, 4, 5\}.$$

To find the cyclic subgroup $\langle 2 \rangle$, find the consecutive multiples of 2, starting at the identity element 0 and stopping when 0 is reached again.

The multiples of 2 in $(\mathbb{Z}_6, +_6)$ are

$$\ldots, 0, 2, 4, 0, \ldots,$$

and 4 is the inverse of 2, so

$$\langle 2 \rangle = \{0, 2, 4\},$$
$$\langle 4 \rangle = \{0, 2, 4\}.$$

Finally, 3 is self-inverse, so

$$\langle 3 \rangle = \{0, 3\}.$$

Again, the orders of the cyclic subgroups agree with the orders of their generators, as expected from Theorem B33.

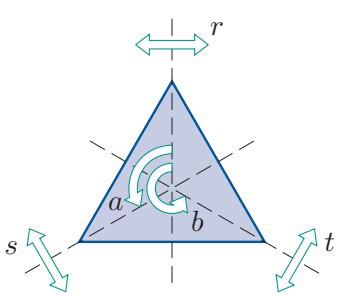


Figure 18 $S(\triangle)$

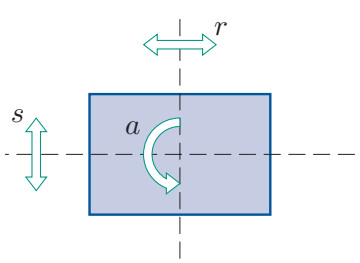


Figure 19 $S(\square)$

Exercise B58

Find the cyclic subgroup generated by each element in each of the following groups.

(a) $S(\triangle)$ (b) $S(\square)$ (c) $(\mathbb{Z}_5^*, \times_5)$ (d) $(\mathbb{Z}_8, +_8)$

(Your working for Exercise B55 should be helpful. The non-identity elements of $S(\triangle)$ and $S(\square)$ are shown in Figures 18 and 19.)

Worked Exercise B26 and Exercise B58 illustrate that one way to find some subgroups of a group is to find its cyclic subgroups.

Notice, however, that different elements of the group can generate the same cyclic subgroup. For example, in $S(\square)$, the elements a and c both generate the subgroup $\{e, a, b, c\}$.

Note also that a group can have subgroups that are not cyclic subgroups. For example, $\{e, b, r, t\}$ is a subgroup of $S(\square)$, as you saw in Worked Exercise B19, but it is not generated by any of the elements of $S(\square)$, as you can see from the solution to Worked Exercise B26(a).

Cyclic subgroups of $S(\bigcirc)$

To end this subsection, let us find some cyclic subgroups of $S(\bigcirc)$, the symmetry group of the disc.

Remember from Unit B1 that the symmetries of the disc are:

r_θ: rotation through an angle θ about the centre, for $\theta \in [0, 2\pi)$

q_θ: reflection in the line through the centre at an angle θ to the horizontal (measured anticlockwise), for $\theta \in [0, \pi)$.

So

$$S(\bigcirc) = \{r_\theta : \theta \in [0, 2\pi)\} \cup \{q_\theta : \theta \in [0, \pi)\}.$$

The identity element of the group $S(\bigcirc)$ is r_0.

Any reflection q_θ is self-inverse, as illustrated in Figure 20, so it has order 2 and generates a cyclic subgroup

$$\langle q_\theta \rangle = \{r_0, q_\theta\}$$

of order 2.

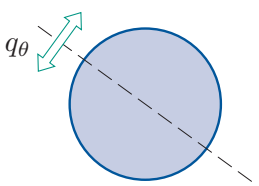


Figure 20 A reflection q_θ

The situation with the rotations in $S(\bigcirc)$ is more complicated. First, let us find a formula for a power of a rotation. If we take a particular rotation r_θ and apply it k times, then the effect is the same as that of applying the rotation $r_{k\theta}$. That is,

$$r_\theta^k = r_{k\theta}.$$

Of course, the angle $k\theta$ may not lie in the interval $[0, 2\pi)$, but $r_{k\theta}$ is equivalent to a rotation through an angle that does lie in this interval.

Some of the rotations in $S(\bigcirc)$ have finite order. For example, for the rotation $r_{2\pi/5}$, the five powers

$$r_{2\pi/5}^0 = r_0,$$
$$r_{2\pi/5}^1 = r_{2\pi/5},$$
$$r_{2\pi/5}^2 = r_{4\pi/5},$$
$$r_{2\pi/5}^3 = r_{6\pi/5},$$
$$r_{2\pi/5}^4 = r_{8\pi/5}$$

are all distinct, as illustrated in Figure 21, and the next power is

$$r_{2\pi/5}^5 = r_{10\pi/5} = r_{2\pi} = r_0,$$

so the powers start repeating. So this rotation has order 5 and generates the following cyclic subgroup of order 5:

$$\langle r_{2\pi/5} \rangle = \{r_0,\ r_{2\pi/5},\ r_{4\pi/5},\ r_{6\pi/5},\ r_{8\pi/5}\}.$$

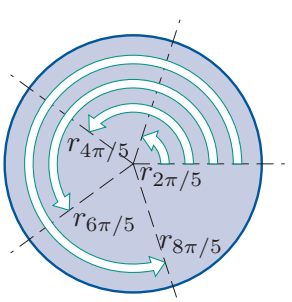


Figure 21 Powers of $r_{2\pi/5}$

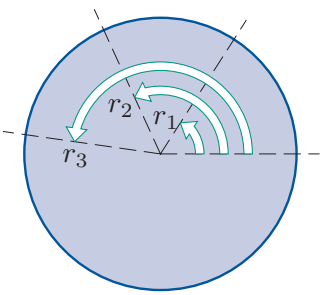


Figure 22 Some powers of r_1

Other rotations have infinite order. For example, consider r_1, the rotation through one radian, which is just over 57°, as illustrated in Figure 22. We have

$$r_1^2 = r_{2\times 1} = r_2,$$
$$r_1^3 = r_{3\times 1} = r_3,$$

and so on. No power of r_1 is equal to the identity symmetry r_0. To see this, we can use the fact that the kth power of r_1 is given by

$$r_1^k = r_{k\times 1} = r_k.$$

So if there *were* an integer k such that $r_1^k = r_0$, then k would be a multiple of 2π, say $k = 2s\pi$ where s is an integer, and this equation gives $\pi = k/(2s)$, which is impossible as π is irrational. So r_1 generates a cyclic subgroup of infinite order.

Exercise B59

Find the order of each of the following cyclic subgroups of $S(\bigcirc)$.

(a) $\langle r_{\pi/4}\rangle$ (b) $\langle r_{\pi/3}\rangle$ (c) $\langle r_{2\pi/7}\rangle$ (d) $\langle r_2\rangle$

3.2 Cyclic groups

In Worked Exercise B26 we found all the cyclic subgroups of the groups $S(\square)$ and $(\mathbb{Z}_6, +_6)$, as follows.

Cyclic subgroups of $S(\square)$	Cyclic subgroups of $(\mathbb{Z}_6, +_6)$
$\langle e\rangle = \{e\}$	$\langle 0\rangle = \{0\}$
$\langle a\rangle = \{e, a, b, c\}$	$\langle 1\rangle = \{0, 1, 2, 3, 4, 5\}$
$\langle b\rangle = \{e, b\}$	$\langle 2\rangle = \{0, 2, 4\}$
$\langle c\rangle = \{e, a, b, c\}$	$\langle 3\rangle = \{0, 3\}$
$\langle r\rangle = \{e, r\}$	$\langle 4\rangle = \{0, 2, 4\}$
$\langle s\rangle = \{e, s\}$	$\langle 5\rangle = \{0, 1, 2, 3, 4, 5\}$
$\langle t\rangle = \{e, t\}$	
$\langle u\rangle = \{e, u\}$	

Notice that $(\mathbb{Z}_6, +_6)$ contains two elements that each generate the whole group:

$$\langle 1\rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6,$$
$$\langle 5\rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6.$$

In contrast, none of the elements of the group $S(\square)$ generates the whole group $S(\square) = \{e, a, b, c, r, s, t, u\}$: each element generates only a proper subgroup.

We make the following definitions.

Definitions

Let G be a group. If there is an element $x \in G$ such that $G = \langle x \rangle$, then G is a **cyclic group**.

If there is no such element, then G is **non-cyclic**.

So $(\mathbb{Z}_6, +_6)$ is a cyclic group, whereas $S(\square)$ is non-cyclic.

The following theorem follows immediately from the fact that a group element of order n generates a cyclic subgroup of order n (Theorem B33(a)).

Theorem B34

Let G be a finite group of order n. Then G is cyclic if and only if G contains an element of order n.

So $(\mathbb{Z}_6, +_6)$ is cyclic because it has order 6 and contains an element of order 6 (namely 1 or 5). On the other hand, $S(\square)$ is non-cyclic because it has order 8 but contains no element of order 8. When you want to show that a group is cyclic, it is sometimes more efficient to use Theorem B34 rather than the definition of a cyclic group.

Exercise B60

Determine which of the following groups are cyclic. (You were asked to find the order of each element of these groups in Exercise B55.)

(a) $S(\triangle)$ (b) $S(\square)$ (c) $(\mathbb{Z}_5^*, \times_5)$ (d) $(\mathbb{Z}_8, +_8)$

The definitions of cyclic and non-cyclic groups apply to both finite and infinite groups. An example of an infinite cyclic group is $(\mathbb{Z}, +)$, because in this group

$$\begin{aligned}\langle 1 \rangle &= \{k \times 1 : k \in \mathbb{Z}\} \\ &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \\ &= \mathbb{Z}.\end{aligned}$$

Since $(\mathbb{Z}, +)$ is generated by 1, it is also generated by -1, the inverse of 1:

$$\begin{aligned}\langle -1 \rangle &= \{k \times (-1) : k \in \mathbb{Z}\} \\ &= \{\ldots, 2, 1, 0, -1, -2, \ldots\} \\ &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \\ &= \mathbb{Z}.\end{aligned}$$

An example of an infinite group that is not cyclic is $(\mathbb{R}^*, \times)$. One way to see that this group is non-cyclic is to use a contradiction argument, as follows. Suppose that $(\mathbb{R}^*, \times)$ *is* cyclic, with generator x. Then, since $-1 \in \mathbb{R}^*$, there is a non-zero integer k such that

$$x^k = -1.$$

It follows that

$$x^k \times x^k = (-1) \times (-1),$$

that is

$$x^{2k} = 1. \tag{2}$$

It follows from this equation that

$$(x^{2k})^{-1} = 1^{-1},$$

that is,

$$x^{-2k} = 1. \tag{3}$$

Since one of $2k$ and $-2k$ must be positive, equations (2) and (3) tell us that there is a positive integer n such that $x^n = 1$. Hence x has finite order. Therefore x does not generate $\mathbb{R}^*$, which is a contradiction.

The theorem below gives a simple property of cyclic groups. You are asked to try to prove it in the next exercise.

Theorem B35

Every cyclic group is abelian.

Exercise B61

Show that if $(G, \circ)$ is a cyclic group, then $(G, \circ)$ is abelian.

Hint: Suppose that $(G, \circ)$ is generated by a. Then every element of G can be expressed as a power of a.

The next theorem gives a less obvious property of cyclic groups. It applies to both finite and infinite groups. The proof of this theorem is quite complicated; if you are interested in it, and have plenty of time, then take the time to read it and understand it, but do not worry about skipping it otherwise. At this stage you are likely to learn more from simpler proofs in group theory.

Theorem B36

Every subgroup of a cyclic group is cyclic.

Proof Let $(G, \circ)$ be a cyclic group, generated by a, and let H be a subgroup of $(G, \circ)$.

If H is the trivial subgroup, then it is cyclic (generated by the identity element). So now suppose that H is not the trivial subgroup. All the elements of H can be expressed as powers of a (because H is a subset of G), and hence H must contain at least one element that can be expressed as a^k where k is *positive*, because H is a subgroup of G and therefore if $a^k \in H$ then also $(a^k)^{-1} = a^{-k} \in H$. Let m be the *smallest* positive integer such that a^m is in H. We will show that a^m generates H.

To do this, we have to show that every element of H can be expressed as a power of a^m. So let h be an element of H. Then $h = a^k$ for some integer k. The Division Theorem, which you met in Unit A2 *Number systems* gives

$$k = qm + r,$$

where q and r are integers, and $0 \leq r < m$. Thus

$$r = k - qm,$$

so, by the index laws for group elements,

$$a^r = a^{k-qm} = a^k \circ (a^m)^{-q}.$$

Now both a^k and a^m are elements of H, and H is a group under $\circ$, so it follows from the equation above that a^r is in H. Hence, since $0 \leq r < m$ and m is the *smallest* positive integer such that a^m is in H, we must have $r = 0$. Thus $k = qm$, and so

$$h = a^k = (a^m)^q.$$

This shows that h can be expressed as a power of a^m, which completes the proof. ■

Earlier in this unit you met some methods for finding some of the subgroups of a symmetry group. In general, finding *all* the subgroups of a finite group is a tricky and time-consuming task. Theorem B36 tells us that the task is much simpler if the group is cyclic: we just have to find all its distinct *cyclic* subgroups. This is illustrated below.

Worked Exercise B27

Find all the subgroups of the group $(\mathbb{Z}_6, +_6)$, writing down a list in which each subgroup appears just once.

Solution

The cyclic subgroups of the group $(\mathbb{Z}_6, +_6)$ (as found in Worked Exercise B26) are as follows.

Remember that an element and its inverse generate the same cyclic subgroup.

$\langle 0 \rangle = \{0\}$,
$\langle 1 \rangle = \langle 5 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$,
$\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$,
$\langle 3 \rangle = \{0, 3\}$.

Since $\langle 1 \rangle = \mathbb{Z}_6$, the group $(\mathbb{Z}_6, +_6)$ is cyclic, and hence all its subgroups are cyclic.

So all the subgroups of $(\mathbb{Z}_6, +_6)$ are included in the list above.

So the subgroups of $(\mathbb{Z}_6, +_6)$ are:

$\{0\}$, $\{0, 2, 4\}$, $\{0, 3\}$, $\mathbb{Z}_6$.

Exercise B62

You saw in Exercise B60 that the two groups below are cyclic, and you were asked to find all their cyclic subgroups in Exercise B58. Find all the subgroups of each group, writing down a list in which each subgroup appears just once.

(a) $(\mathbb{Z}_5^*, \times_5)$ (b) $(\mathbb{Z}_8, +_8)$

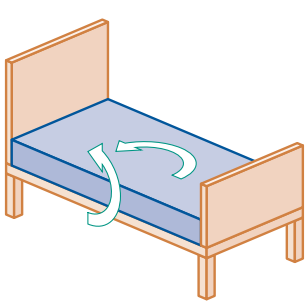


Figure 23 Turning a mattress

Group theory and mattress turning

There is a connection between the theory of cyclic groups and the question of how you turn your mattress. Some mattresses need to be turned, every few months, such that the turning includes both head to foot rotating, and top to bottom flipping, as illustrated in Figure 23. There are four possible positions in which such a mattress can be placed on the bed, so the group of direct symmetries of the mattress (when the mattress is regarded as a perfect cuboid, of course) has order 4. It would be nice if there were a particular mattress turning move, such that if you used this move every time you turned the mattress, then the mattress would cycle through its four possible positions in turn. Unfortunately, there is no such move – this is because the group of direct symmetries of the mattress is not cyclic!

Some more modern mattresses need to be rotated head to foot only, and should not be flipped over. So they have only two possible positions; these correspond to a subgroup of order 2 of the group of direct symmetries of the mattress. Every group of order 2 is cyclic (generated by the single element that is not the identity element), so with such a mattress you *can* make the same move each time, and have the mattress cycle through its two possible positions.

3.3 Cyclic groups from modular arithmetic

In this subsection we focus on cyclic groups that arise from modular arithmetic.

Additive cyclic groups from modular arithmetic

In the previous subsection you saw that the additive groups $(\mathbb{Z}_6, +_6)$ and $(\mathbb{Z}_8, +_8)$ are cyclic groups. Each of these cyclic groups is generated by the integer 1, as shown in Figure 24.

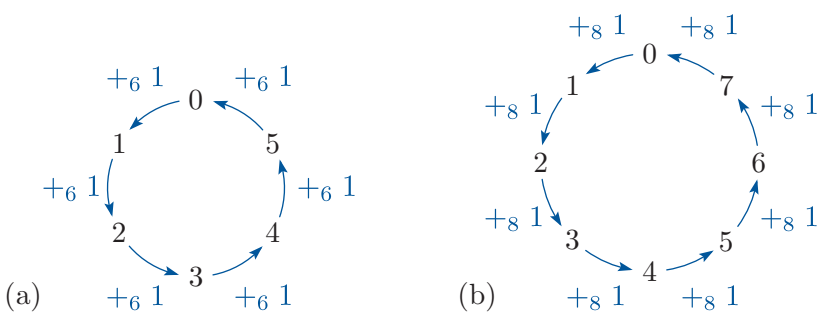


Figure 24 The cycle of multiples of 1 in (a) $(\mathbb{Z}_6, +_6)$ (b) $(\mathbb{Z}_8, +_8)$

In general, for any positive integer n, the cycle of multiples of 1 in $(\mathbb{Z}_n, +_n)$ contains each element of $\mathbb{Z}_n$, and hence generates the whole group $(\mathbb{Z}_n, +_n)$, as shown in Figure 25.

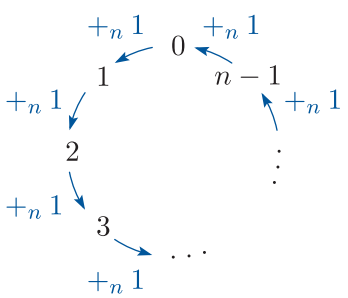


Figure 25 The cycle of multiples of 1 in $(\mathbb{Z}_n, +_n)$

So we can state the following result.

Theorem B37

For each integer $n \geq 2$, the group $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n. It is generated by the integer 1.

In general the integer 1 is not the only generator of the cyclic group $(\mathbb{Z}_n, +_n)$. The inverse of 1 (which is $n - 1$, since $1 +_n (n - 1) = 0$) also generates the group, as you know from Subsection 3.1, and usually some other integers do too, as illustrated in the next exercise.

Exercise B63

By looking back at your answer (or the solution) to Exercise B58(d), write down all the generators of the cyclic group $(\mathbb{Z}_8, +_8)$.

In Subsection 3.4 you will meet a result that tells you exactly which elements of $\mathbb{Z}_n$ are generators of the cyclic group $(\mathbb{Z}_n, +_n)$, for any $n \geq 2$.

Multiplicative cyclic groups from modular arithmetic

In Theorem B9 of Unit B1 you saw that for all integers $n \geq 2$, the set U_n of integers in $\mathbb{Z}_n$ coprime to n is a group under $\times_n$. The next two activities demonstrate that the group $(U_n, \times_n)$ may or may not be cyclic.

Exercise B64

(a) Write down the elements of the group $(U_{18}, \times_{18})$.

(b) Find all the cyclic subgroups of this group.

(c) Deduce that $(U_{18}, \times_{18})$ is cyclic, and list all its generators.

Exercise B65

Use the solution to Exercise B56(a) to show that $(U_{20}, \times_{20})$ is not a cyclic group.

Since the group $(U_{18}, \times_{18})$ is cyclic it is straightforward to write down all of its subgroups, as they must all be cyclic, by Theorem B36. In contrast, the non-cyclic group $(U_{20}, \times_{20})$ may have some subgroups that are not cyclic.

Exercise B66

Using your answer to Exercise B64, write down all the subgroups of the group $(U_{18}, \times_{18})$, giving a list in which each subgroup appears just once.

Exercise B67

Show that $(\{1, 9, 11, 19\}, \times_{20})$ is a subgroup of $(U_{20}, \times_{20})$, but that it is not a cyclic subgroup.

3.4 The group $(\mathbb{Z}_n, +_n)$

In this subsection we will look more closely at the additive cyclic group $(\mathbb{Z}_n, +_n)$, $n \geq 2$. In particular we will look at how we can determine the orders of its elements, and how we can efficiently find its subgroups.

Orders of elements of $(\mathbb{Z}_n, +_n)$

We have found the orders of all the elements in several of the groups $(\mathbb{Z}_n, +_n)$, as follows.

$(\mathbb{Z}_6, +_6)$

Element	0	1	2	3	4	5
Order	1	6	3	2	3	6

$(\mathbb{Z}_8, +_8)$

Element	0	1	2	3	4	5	6	7
Order	1	8	4	8	2	8	4	8

$(\mathbb{Z}_{12}, +_{12})$

Element	0	1	2	3	4	5	6	7	8	9	10	11
Order	1	12	6	4	3	12	2	12	3	4	6	12

These results were obtained in Worked Exercise B24, Exercise B55(d) and Exercise B56(b), respectively. In the next exercise you are asked to find the orders of the elements in another group $(\mathbb{Z}_n, +_n)$. In this case the value of n is prime.

Exercise B68

Find the order of each element of the group $(\mathbb{Z}_5, +_5)$.

The order of an integer m in a cyclic group $(\mathbb{Z}_n, +_n)$ must be related to the integers m and n – but how? The examples above and the solution to Exercise B68 seem to suggest that the order of the integer m in $(\mathbb{Z}_n, +_n)$ is always a factor of n, but it is hard to spot a pattern that might suggest what the exact relationship is. In fact, the relationship is as follows.

Theorem B38 Order of an element of $(\mathbb{Z}_n, +_n)$

Let m be a non-zero element of the group $(\mathbb{Z}_n, +_n)$. Then m has order n/d, where d is the highest common factor (HCF) of m and n.

This theorem is simple to state, and it has a number of important consequences, but unfortunately it is quite complicated to prove. A proof is provided at the end of this subsection for those who are interested and have plenty of time, but you can skip it if you prefer.

Notice that the theorem tells us how to work out the order of each *non-zero* integer in any group $(\mathbb{Z}_n, +_n)$. However, we already know that the order of the integer 0 in $(\mathbb{Z}_n, +_n)$ is 1, since 0 is the identity element in $(\mathbb{Z}_n, +_n)$.

Worked Exercise B28

Use Theorem B38 to find the order of the integer 8 in $(\mathbb{Z}_{12}, +_{12})$.

Solution

The HCF of 8 and 12 is 4, so the order of 8 in $(\mathbb{Z}_{12}, +_{12})$ is $12/4 = 3$.

Exercise B69

Using Theorem B38, determine the order of each integer in each of the following groups. Check that your answer to part (a) agrees with the table of orders of elements of $(\mathbb{Z}_6, +_6)$ at the start of this subsection, and that your answer to part (b) agrees with your answer to Exercise B68.

(a) $(\mathbb{Z}_6, +_6)$ (b) $(\mathbb{Z}_5, +_5)$

In Exercise B69(b) (and also in Exercise B68 earlier) you should have found that the order of every non-zero integer in $(\mathbb{Z}_5, +_5)$ is 5. This is an instance of the following corollary to Theorem B38.

Corollary B39

Let m be a non-zero element of the group $(\mathbb{Z}_p, +_p)$, where p is prime. Then m has order p.

Proof Since p is prime, the highest common factor of m and p is 1. Hence, by Theorem B38, the order of m is $p/1 = p$. ■

Here is another enlightening corollary of Theorem B38. It tells us which elements of a group $(\mathbb{Z}_n, +_n)$ are generators of $(\mathbb{Z}_n, +_n)$.

Corollary B40 Generators of $(\mathbb{Z}_n, +_n)$

Let $m \in \mathbb{Z}_n$. Then m is a generator of the group $(\mathbb{Z}_n, +_n)$ if and only if m is coprime to n.

Proof If $m = 0$, then m is not a generator of $(\mathbb{Z}_n, +_n)$, and m is not coprime to n, so the statement holds for this value of m.

Now suppose that m is any non-zero integer in $\mathbb{Z}_n$, and let d be the highest common factor of m and n. By Theorem B38, m is a generator of $(\mathbb{Z}_n, +_n)$ if and only if

$$\frac{n}{d} = n,$$

that is,

$$d = 1.$$

This equation holds if and only if m and n are coprime. This completes the proof. ■

You saw an instance of Corollary B40 in Exercise B63, where it was found that the generators of $(\mathbb{Z}_8, +_8)$ are 1, 3, 5 and 7; these are the elements of $\mathbb{Z}_8$ that are coprime to 8. As another example, notice that it follows from the solution to Exercise B68 that all the non-zero elements of $\mathbb{Z}_5$ generate $(\mathbb{Z}_5, +_5)$; all the non-zero elements of $\mathbb{Z}_5$ are coprime to 5, since 5 is prime.

Notice that Corollary B40 tells us that the generators of the group $(\mathbb{Z}_n, +_n)$ are the elements of the set U_n.

Exercise B70

For each of the following groups, write down all the generators of the group.

(a) $(\mathbb{Z}_7, +_7)$ (b) $(\mathbb{Z}_{10}, +_{10})$

Subgroups of $(\mathbb{Z}_n, +_n)$

We can use Theorem B38 to prove a theorem that describes exactly what the subgroups of $(\mathbb{Z}_n, +_n)$ are, for any integer $n \geq 2$. Before you see this theorem, let us look at two examples of groups $(\mathbb{Z}_n, +_n)$, namely $(\mathbb{Z}_6, +_6)$ and $(\mathbb{Z}_8, +_8)$, and find their subgroups.

By the solution to Worked Exercise B26, the distinct cyclic subgroups of the group $(\mathbb{Z}_6, +_6)$ are

$$\langle 0 \rangle = \{0\}, \quad \text{of order 1,}$$
$$\langle 3 \rangle = \{0, 3\}, \quad \text{of order 2,}$$
$$\langle 2 \rangle = \{0, 2, 4\}, \quad \text{of order 3,}$$
$$\langle 1 \rangle = \mathbb{Z}_6, \quad \text{of order 6.}$$

There are no other cyclic subgroups of $(\mathbb{Z}_6, +_6)$, because the subgroup generated by each other element of $\mathbb{Z}_6$ is the same as one of the subgroups above. For example,

$$\langle 4 \rangle = \{0, 4, 2\} = \{0, 2, 4\} = \langle 2 \rangle.$$

Also, as you saw in Worked Exercise B27, the list above contains *all* the subgroups of $(\mathbb{Z}_6, +_6)$, because $(\mathbb{Z}_6, +_6)$ is cyclic and so all its subgroups are cyclic, by Theorem B36.

The list shows that $(\mathbb{Z}_6, +_6)$ has exactly one cyclic subgroup of order q for each positive factor q of 6, and no other subgroups.

Similarly, by the solution to Exercise B62(b), the complete list of subgroups of the group $(\mathbb{Z}_8, +_8)$ is as follows:

$\langle 0 \rangle = \{0\}$, of order 1,
$\langle 4 \rangle = \{0, 4\}$, of order 2,
$\langle 2 \rangle = \{0, 2, 4, 6\}$, of order 4,
$\langle 1 \rangle = \mathbb{Z}_8$, of order 8.

This list shows that $(\mathbb{Z}_8, +_8)$ has exactly one cyclic subgroup of order q for each positive factor q of 8, and no other subgroups.

In general, the following result holds.

Theorem B41 Subgroups of $(\mathbb{Z}_n, +_n)$

The group $(\mathbb{Z}_n, +_n)$ has exactly one cyclic subgroup of order q for each positive factor q of n, and no other subgroups.

- The subgroup of order 1 is generated by 0.
- For each other factor q of n, the subgroup of order q is generated by d, where $qd = n$.

Proof Since $(\mathbb{Z}_n, +_n)$ is a cyclic group, all its subgroups are cyclic, by Theorem B36.

There is a cyclic subgroup of order 1, namely the subgroup generated by 0. Now let q be any factor of n other than 1, and let d be given by $qd = n$. Then d is a factor of n, so the highest common factor of d and n is d, and hence, by Theorem B38, d generates a cyclic subgroup of order $n/d = q$.

So we have described one cyclic subgroup of order q for each positive factor q of n.

We now show that there are no further cyclic subgroups of $(\mathbb{Z}_n, +_n)$. Let m be any non-zero integer in $\mathbb{Z}_n$, and consider the cyclic subgroup $\langle m \rangle$. Let d be the highest common factor of m and n. Then m is a multiple of d, so $m \in \langle d \rangle$ and hence $\langle m \rangle$ is a subgroup of $\langle d \rangle$, by Theorem B32. But, by Theorem B38, the subgroups $\langle m \rangle$ and $\langle d \rangle$ have the same order, namely n/d, so they must be equal. Hence the subgroup $\langle m \rangle$ is the same as one of the subgroups already described. So there are no further cyclic subgroups. ■

Exercise B71

Using Theorem B41, find all the subgroups of each of the following groups. Give a list in which each subgroup appears exactly once.

(a) $(\mathbb{Z}_{12}, +_{12})$ (b) $(\mathbb{Z}_9, +_9)$ (c) $(\mathbb{Z}_{11}, +_{11})$

Unfortunately, finding all the subgroups of a group is usually a far more difficult task than it is for one of the groups $(\mathbb{Z}_n, +_n)$.

Connections between cyclic groups

To conclude our discussion of cyclic groups, let us compare two particular cyclic groups of order 4.

The group $(S^+(\square), \circ)$ of direct (that is, rotational) symmetries of the square is a cyclic group of order 4. It is generated by a, the rotation through $\pi/2$, as shown in Figure 26. (The non-identity elements of $S^+(\square)$ are illustrated in Figure 27.)

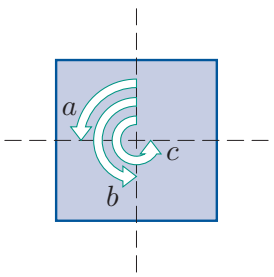


Figure 27 $S^+(\square)$

$$S^+(\square) = \{e, a, b, c\}$$

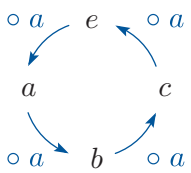


Figure 26 The cyclic group $(S^+(\square), \circ)$

The group $(\mathbb{Z}_4, +_4)$ is a cyclic group of order 4 that is generated by the element 1, as shown in Figure 28.

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

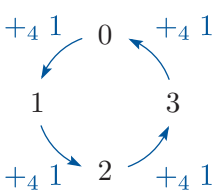


Figure 28 The cyclic group $(\mathbb{Z}_4, +_4)$

The diagrams in Figures 26 and 28 are very similar. If we take the diagram in Figure 26 and replace the elements e, a, b and c by 0, 1, 2 and 3 using the 'matching'

$$\begin{array}{cccc} e & a & b & c \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & 3 \end{array},$$

and also replace the operation $\circ$ by the operation $+_4$, then we obtain the diagram in Figure 28. So, *structurally*, these two groups are identical: it is just the names of the elements and the names of the binary operations that differ. Just as the element a generates the first group $(S^+(\square), \circ)$, so the corresponding element, 1, generates the second group $(\mathbb{Z}_4, +_4)$; and just as the element b in $(S^+(\square), \circ)$ has order 2, so its corresponding element, 2, in $(\mathbb{Z}_4, +_4)$ has order 2. Similarly, just as e is the identity element of the first group, so its corresponding element, 0, is the identity element of the second group. Any other cyclic group of order 4 has exactly the same structure as these two groups.

In the same way, for any positive integer n, all the cyclic groups of order n have exactly the same structure as each other.

Proof of Theorem B38 (optional)

Finally in this subsection, here is a proof of Theorem B38, as promised. It will not be assessed: read it if you are interested and have plenty of time – skip it otherwise. The theorem is as follows.

Theorem B38

Let m be a non-zero element of the group $(\mathbb{Z}_n, +_n)$. Then m has order n/d, where d is the highest common factor of m and n.

We start with a lemma that is a particular case of Theorem B38, namely the case where m is a factor of n. This case is much easier to prove.

Lemma B42

Let m be a non-zero element of the group $(\mathbb{Z}_n, +_n)$. If m is a factor of n, then m has order n/m.

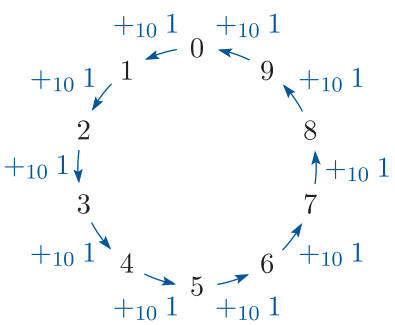


Figure 29 The cycle of multiples of 1 in $(\mathbb{Z}_{10}, +_{10})$

To see why this lemma holds, consider, for example, the integer 2 in $(\mathbb{Z}_{10}, +_{10})$. Repeatedly adding 2 in $\mathbb{Z}_{10}$ is the same as moving 2 places at a time round the cycle in Figure 29. If we start from 0 and add 2 a total of $10/2 = 5$ times then we get back to 0, whereas if we add 2 any fewer than 5 times then we do not get back to 0. So the order of 2 in $(\mathbb{Z}_{10}, +_{10})$ is 5.

Generalising this argument gives the following proof of Lemma B42.

Proof of Lemma B42 Suppose that m is a factor of n. Repeatedly adding m in $(\mathbb{Z}_n, +_n)$ is the same as moving m places at a time round the cycle in Figure 30. If we start from 0 and add m a total of n/m times then we get back to 0, whereas if we add m any fewer than n/m times then we do not get back to 0. Hence the order of m in $(\mathbb{Z}_n, +_n)$ is n/m. ■

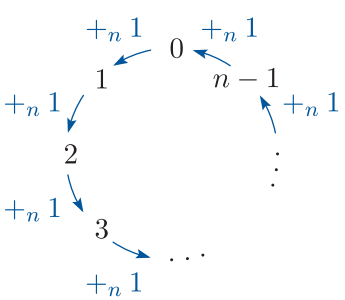


Figure 30 The cycle of multiples of 1 in $(\mathbb{Z}_n, +_n)$

Now here is the proof of Theorem B38. You will see that in this proof we use both the result of Lemma B42, and the ideas used in the proof of Lemma B42.

Proof of Theorem B38 Let m be a non-zero integer in $\mathbb{Z}_n$, and let d be the highest common factor of m and n. Then m/d and n/d are coprime integers. Also, since d is a factor of n, the order of d is n/d, by Lemma B42.

We have to show that the order of m is also n/d. First we show that the order of m is *at most* n/d. Consider the cycle of multiples of 1 in $(\mathbb{Z}_n, +_n)$, shown in Figure 30.

Suppose that we start from 0 and move round m places at a time, a total of n/d times. This is the same as starting from 0 and moving round a total of mn/d places. Since m/d is an integer, the number mn/d is a multiple of n, so we end up at 0. Hence the order of m is indeed at most n/d.

Now we show that the order of m cannot be less than n/d. We use a contradiction argument. Suppose that the order of m is r, where $1 \leq r < n/d$. Then if we start from 0 in the cycle in Figure 30 and move round m places at a time, a total of r times, we end up at 0. Hence

$$rm = kn \tag{4}$$

for some natural number k. Dividing both sides of this equation by d and rearranging slightly, we obtain

$$r\frac{m}{d} = k\frac{n}{d}.$$

Now remember that m/d and n/d are coprime integers. The equation above tells us that m/d is a factor of $k(n/d)$, and hence, since m/d is coprime to n/d, it follows that m/d is a factor of k. Therefore the number $k/(m/d)$, that is, kd/m, is an integer.

If we now go back to equation (4), multiply it through by d and divide it through by m, then we obtain

$$rd = \frac{kd}{m}n.$$

Thus rd is an integer multiple of n. So if we start from 0 in the cycle in Figure 30 and move round d places at a time, a total of r times, then we end up at 0. But $1 \leq r < n/d$, so this contradicts the fact that the order of d is n/d. Thus the order of m cannot be less than n/d.

This completes the proof that the order of m is n/d. ■

4 Isomorphisms

Near the end of the previous section, just before the proof of Theorem B38, it was pointed out that the cyclic groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$ of order 4 are structurally identical, and that in fact all the cyclic groups of any particular order are structurally identical to each other. In this section we will explore the idea of structurally identical groups for groups in general, both cyclic and non-cyclic.

4.1 Cayley tables of groups of orders 4 and 6

One way to compare the structures of two finite groups is to look at their Cayley tables. In this subsection we will do this for some groups of orders 4 and 6.

Cayley tables of groups of order 4

Let us start by looking at the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$ again, this time comparing their structures by looking at their Cayley tables, which are as follows.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$(S^+(\square), \circ)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_4, +_4)$

You can see that if we take the Cayley table of $(S^+(\square), \circ)$, and replace the elements e, a, b and c by 0, 1, 2 and 3 using the same matching as before, namely

$$\begin{array}{cccc} e & a & b & c \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & 3 \end{array},$$

and also replace the operation $\circ$ by the operation $+_4$, then we obtain the Cayley table of $(\mathbb{Z}_4, +_4)$. This shows that the two groups are structurally identical, as we also found in Subsection 3.4.

The Cayley table of $(\mathbb{Z}_4, +_4)$ can be obtained from the Cayley table of $(S^+(\square), \circ)$ by 'renaming' the elements because the two Cayley tables have exactly the same pattern. They both have the pattern of bottom left to top right diagonal stripes shown in Figure 31.

Figure 31 The pattern of the Cayley tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$

Now let us look at another group of order 4, and try to determine whether it has the same structure as $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$. The group $(\mathbb{Z}_5^*, \times_5)$ has the following Cayley table.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}_5^*, \times_5)$

The pattern in this Cayley table, shown in Figure 32, is different from the pattern in the Cayley tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$.

Figure 32 The pattern of the Cayley table of $(\mathbb{Z}_5^*, \times_5)$

However, it is possible to rearrange the Cayley table of $(\mathbb{Z}_5^*, \times_5)$ to make it have the same pattern as the Cayley tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$, that is, the pattern of diagonal stripes in Figure 31. One way to do this is to interchange the positions of the elements 3 and 4 in the borders of the table (this must be done in both borders) and rearrange the entries in the body of the table accordingly.

To rearrange the entries in the body of the table, we can either just fill them in again using the rearranged table borders, or we can take the original table, interchange the last two columns to obtain an intermediate table, and then interchange the last two rows of this intermediate table to obtain the new table, as shown below.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

original table

$\longrightarrow$ swap columns 3, 4

$\times_5$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
3	3	1	2	4
4	4	3	1	2

intermediate table

$\longrightarrow$ swap rows 3, 4

$\times_5$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

rearranged table

Either way, we end up with the rearranged Cayley table of $(\mathbb{Z}_5^*, \times_5)$ shown on the right above. This table has the same pattern of diagonal stripes as the Cayley tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$. Hence the group $(\mathbb{Z}_5^*, \times_5)$ is structurally identical to the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$.

Exercise B72

For each of the following pairs of groups, write down a matching between the elements of the first group and the elements of the second group, such that if the elements in the Cayley table of the first group are replaced according to this matching, then the Cayley table of the second group is obtained.

(a) $(S^+(\square), \circ)$ and $(\mathbb{Z}_5^*, \times_5)$ (b) $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \times_5)$

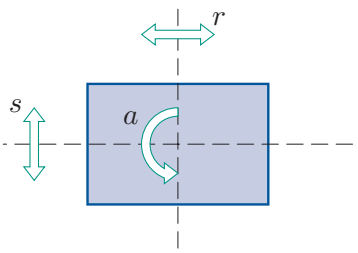


Figure 33 $S(\square)$

It is important to remember that when you rearrange the entries in the borders of a Cayley table, you must rearrange both borders in the same way. In a Cayley table the entries in the two borders must be in the same order.

The three groups of order 4 that we have looked at so far in this subsection all have Cayley tables that can be rearranged into the pattern of diagonal stripes shown in Figure 31. Let us now look at two more groups of order 4, and try to determine whether their Cayley tables can also be rearranged into this pattern. We will look at the symmetry group of the rectangle, $(S(\square), \circ)$, and the group $(U_8, \times_8)$. The non-identity elements of $S(\square)$ are shown in Figure 33. Remember that U_8 is the set of integers in $\mathbb{Z}_8$ that are coprime to 8, that is, $U_8 = \{1, 3, 5, 7\}$. The Cayley tables of these two groups are as follows.

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

$(S(\square), \circ)$

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$(U_8, \times_8)$

These two Cayley tables do not currently have the pattern of diagonal stripes. They do, however, have the same pattern as each other, shown in Figure 34, so the groups $(S(\square), \circ)$ and $(U_8, \times_8)$ are structurally identical to each other.

Figure 34 The pattern of the Cayley tables of $(S(\square), \circ)$ and $(U_8, \times_8)$

Figure 35 The pattern (diagonal stripes) of the Cayley tables of $(S^+(\square), \circ)$, $(\mathbb{Z}_4, +_4)$ and $\mathbb{Z}_5^*$

To determine whether these two groups are also structurally identical to the first three groups that we looked at in this subsection, we need to find out whether their Cayley tables can be rearranged into the pattern of diagonal stripes in Figure 31, which is repeated in Figure 35. Now, notice that in the pattern of diagonal stripes, the main diagonal (the diagonal from top left to bottom right) contains two different elements, each appearing twice. However, in the groups $(S(\square), \circ)$ and $(U_8, \times_8)$, all the elements are self-inverse, so no matter how we rearrange the borders of their Cayley tables, the four cells on the main diagonal will contain four occurrences of the identity element. So the Cayley tables of $(S(\square), \circ)$ and $(U_8, \times_8)$ cannot be rearranged into the pattern of diagonal stripes in Figure 35.

Thus we have found two different structures for groups of order 4, given by the patterns shown in Figure 36.

Figure 36 The patterns of the Cayley tables of $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$, respectively

It turns out that, for *any* group of order 4, its Cayley table can be rearranged (if necessary) to make it have one of the two patterns in Figure 36. So every group of order 4 has the same structure as one of the groups $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$. You will see a proof of this fact in Unit B4 *Lagrange's Theorem and small groups*.

Notice that both of the patterns in Figure 36 are symmetric with respect to the main diagonal, so every group of order 4 is abelian.

Exercise B73

For each of the following groups of order 4, write down its Cayley table and determine whether it has the same structure as $(\mathbb{Z}_4, +_4)$ or $(S(\square), \circ)$.

(a) $(U_{12}, \times_{12})$ (b) $(U_{10}, \times_{10})$

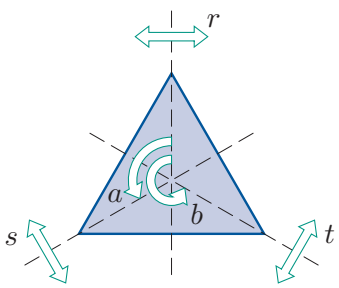


Figure 37 $S(\triangle)$

Cayley tables for groups of order 6

We now look briefly at groups of order 6. Consider the groups $(\mathbb{Z}_6, +_6)$ and $(S(\triangle), \circ)$, both of which have order 6. The non-identity elements of $S(\triangle)$ are shown in Figure 37. The Cayley tables of the two groups are as follows.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$(\mathbb{Z}_6, +_6)$

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$(S(\triangle), \circ)$

These Cayley tables have the patterns shown in Figure 38.

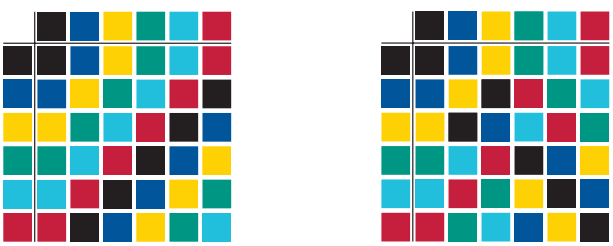


Figure 38 The patterns of the Cayley tables of $(\mathbb{Z}_6, +_6)$ and $(S(\triangle), \circ)$, respectively

Notice that in the pattern of the Cayley table of $(\mathbb{Z}_6, +_6)$, the main diagonal contains three different elements, each appearing twice. However, the group $(S(\triangle), \circ)$ has four self-inverse elements, so no matter how we arrange the borders of its Cayley table, the main diagonal will contain four occurrences of the identity element e. Hence it is not possible to rearrange the Cayley table of $(S(\triangle), \circ)$ into the pattern of the Cayley table of $(\mathbb{Z}_6, +_6)$, and therefore these two groups have different structures.

Thus we have found two different structures for groups of order 6, as given by the patterns shown in Figure 38. It turns out that for any group of order 6, its Cayley table can be rearranged (if necessary) to make it have one of the two patterns in Figure 38. In other words, every group of order 6 has the same structure as one of the groups $(\mathbb{Z}_6, +_6)$ and $(S(\triangle), \circ)$. You will see a proof of this fact in Unit B4.

Notice that the pattern on the left in Figure 38 is symmetric with respect to the main diagonal, so a group with this pattern is an abelian group. In contrast, a group with the pattern on the right is non-abelian.

Notice also that the Cayley table of $(\mathbb{Z}_6, +_6)$ has a pattern of diagonal stripes similar to that of the Cayley table of $(\mathbb{Z}_4, +_4)$. In general, for any integer $n \geq 2$, the Cayley table of $(\mathbb{Z}_n, +_n)$ has a pattern of bottom left to top right diagonal stripes when the elements in the borders are listed in the natural order.

4.2 Isomorphic groups

In this subsection we will formalise exactly what it means for two groups to be 'structurally identical' to each other. We will initially consider finite groups, as we did in the last subsection.

You have seen that two finite groups have the same structure if there is a 'matching' between the elements of the two groups such that when we replace all the elements in a Cayley table for one group using this matching, then we obtain a Cayley table for the other group.

For example, the two groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_5^*, \times_5)$ have the same structure because, as you should have found in Exercise B72(a), if we take a Cayley table of $(S^+(\square), \circ)$ and replace the elements e, a, b and c of $S^+(\square)$ by the elements 1, 2, 3 and 4 of $\mathbb{Z}_5^*$ using the matching

$$\begin{array}{cccc} e & a & b & c \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 4 & 3 \end{array},$$

then we obtain a Cayley table for $(\mathbb{Z}_5^*, \times_5)$:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$(S^+(\square), \circ)$

$\longrightarrow$

$\times_5$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

$(\mathbb{Z}_5^*, \times_5)$

It does not matter here that the elements in the borders of the Cayley table for $(\mathbb{Z}_5^*, \times_5)$ are not listed in the usual order: all that matters is that the table is a correct Cayley table for $(\mathbb{Z}_5^*, \times_5)$.

It is helpful to think of a matching between the elements of two groups as a mapping, say ϕ, from the first group to the second. For example, for the two groups above we have the mapping

$$\begin{aligned} \phi : S^+(\square) &\longrightarrow \mathbb{Z}_5^* \\ e &\longmapsto 1 \\ a &\longmapsto 2 \\ b &\longmapsto 4 \\ c &\longmapsto 3. \end{aligned}$$

If a mapping ϕ from one group to another is to transform a Cayley table for the first group into a Cayley table for the second group, then it must match up *all* the elements of the two groups *one-to-one*. In other words, it must be a one-to-one and onto mapping (that is, a *one-to-one correspondence*). It must also have a further property.

To understand why a further property is necessary, suppose that we replace the elements in the Cayley table for the group $(S^+(\square), \circ)$ by the elements of the group $(\mathbb{Z}_5^*, \times_5)$ using the following one-to-one and onto mapping:

$$\begin{aligned} \phi : S^+(\square) &\longrightarrow \mathbb{Z}_5^* \\ e &\longmapsto 2 \\ a &\longmapsto 3 \\ b &\longmapsto 4 \\ c &\longmapsto 1. \end{aligned}$$

This has the following effect:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$(S^+(\square), \circ)$

$\longrightarrow$

	2	3	4	1
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3
1	1	2	3	4

You can see that although we have obtained a table whose entries are the elements of the group $(\mathbb{Z}_5^*, \times_5)$, *it is not a correct Cayley table for* $(\mathbb{Z}_5^*, \times_5)$. For example, $2 \times_5 2 = 4$, but the cell in the table that should contain the composite $2 \times_5 2$ actually contains the element 2.

So if a mapping ϕ from one group to another is to have the effect of transforming a Cayley table for one group into a Cayley table for another group, then not only must it be one-to-one and onto, but it must also have a further property that ensures that the resulting Cayley table is correct.

To see what this property must be, consider two abstract finite groups, $(G, \circ)$ and $(H, *)$, say. Suppose that we take a Cayley table for $(G, \circ)$ and replace all the elements using a one-to-one and onto mapping $\phi : G \longrightarrow H$. Consider any two elements x and y of G, and their composite $x \circ y$ in the Cayley table for $(G, \circ)$, as illustrated on the left below. In the transformed table, these three elements are replaced by $\phi(x)$, $\phi(y)$ and $\phi(x \circ y)$, as illustrated on the right.

$\circ$	$\cdots$	y	$\cdots$
$\vdots$		$\vdots$	
x	$\cdots$	$x \circ y$	$\cdots$
$\vdots$		$\vdots$	

$(G, \circ)$

$\longrightarrow$

$*$	$\cdots$	$\phi(y)$	$\cdots$
$\vdots$		$\vdots$	
$\phi(x)$	$\cdots$	$\phi(x \circ y)$	$\cdots$
$\vdots$		$\vdots$	

$(H, *)$

If the table obtained is to be a correct Cayley table for $(H, *)$, then the entry in the cell with row label $\phi(x)$ and column label $\phi(y)$ must be equal to $\phi(x) * \phi(y)$, so we must have

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

This applies to *any* elements x and y of G, so the property that we need the mapping ϕ to have is

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{for all } x, y \in G. \tag{5}$$

So saying that two finite groups $(G, \circ)$ and $(H, *)$ have the same structure is the same as saying that there exists a one-to-one and onto mapping ϕ with property (5).

This also applies to *infinite* groups; the only difference is that we cannot write down Cayley tables for such groups.

The term that we use in group theory to describe groups as 'structurally identical' is *isomorphic*. So we make the following definition.

Definition

Two groups $(G, \circ)$ and $(H, *)$ are **isomorphic** if there exists a mapping $\phi : G \longrightarrow H$ with the following properties.

(a) ϕ is one-to-one and onto.

(b) For all $x, y \in G$,

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

Such a mapping ϕ is called an **isomorphism**.

We use the symbol $\cong$ to denote the relation 'is isomorphic to'. That is, we write

$$(G, \circ) \cong (H, *)$$

to assert that the groups $(G, \circ)$ and $(H, *)$ are isomorphic.

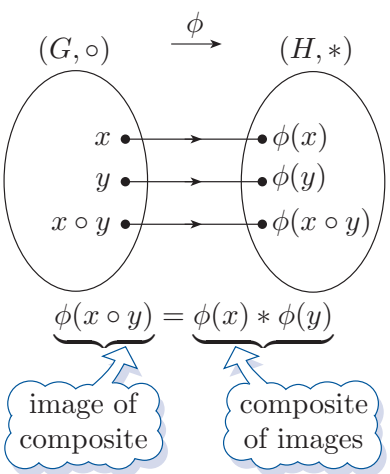


Figure 39 An isomorphism ϕ

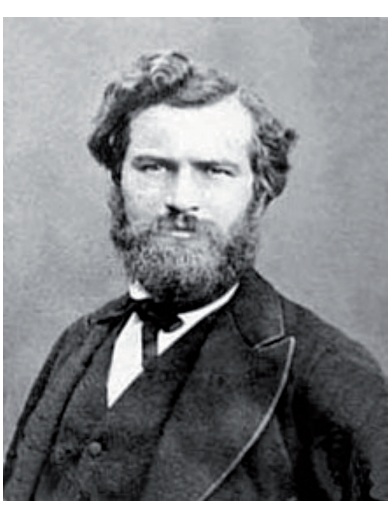
This definition is illustrated in Figure 39.

You have seen that we sometimes write a group $(G, \circ)$ simply as G, when the group operation is understood from the context. Accordingly, we sometimes write $(G, \circ) \cong (H, *)$ simply as $G \cong H$.

Also, we often write an isomorphism $\phi : G \longrightarrow H$ as $\phi : (G, \circ) \longrightarrow (H, *)$, to indicate the binary operations of the two groups G and H.

Remember that, informally, two groups are isomorphic if they have exactly the same structure, even though their elements and binary operation may be different. An isomorphism maps each element of one group to an element 'that has the same role' in the structure of the other group.

The term *isomorphism* was introduced into group theory by the French mathematician Camille Jordan (1838–1922) in his classic treatise *Traité des substitutions et des équations algébriques* (*Treatise on Substitutions and Algebraic Equations*) of 1870, the book in which many modern notions of group theory first appear. The term was used earlier in crystallography.



Camille Jordan

Here is a simple property of isomorphic groups.

Theorem B43

If two groups $(G, \circ)$ and $(H, *)$ are isomorphic, then either $(G, \circ)$ and $(H, *)$ are both finite, with the same order, or $(G, \circ)$ and $(H, *)$ are both infinite.

Proof This follows from the fact that if G and H are isomorphic, then the elements of G can be matched one-to-one with the elements of H. ■

Thus, for example, a group of order 4 cannot be isomorphic to a group of order 6, and a finite group cannot be isomorphic to an infinite group.

The next theorem states some important basic properties of isomorphic groups. These properties are stated in terms of ideas that you met in Unit A3 *Mathematical language*, namely an *equivalence relation* and its constituent properties *reflexivity*, *symmetry* and *transitivity*.

Theorem B44

The relation 'is isomorphic to' is an equivalence relation on the collection of all groups. That is, the following three properties hold.

Reflexivity Every group is isomorphic to itself.

Symmetry For any groups $(G, \circ)$ and $(H, *)$, if $(G, \circ)$ is isomorphic to $(H, *)$, then $(H, *)$ is isomorphic to $(G, \circ)$.

Transitivity For any groups $(G, \circ)$, $(H, *)$ and $(K, \triangle)$, if $(G, \circ)$ is isomorphic to $(H, *)$ and $(H, *)$ is isomorphic to $(K, \triangle)$, then $(G, \circ)$ is isomorphic to $(K, \triangle)$.

You can see that the properties in the theorem hold, because to say that two groups are isomorphic means that they have the same structure; if you replace the words 'is isomorphic to' by the words 'has the same structure as', then the properties become almost obvious. The properties can be proved formally using the definition of isomorphic groups given above, but the proofs are not included here.

Since isomorphism is an equivalence relation, the collection of all groups can be partitioned into equivalence classes, which we call **isomorphism classes**, such that two groups belong to the same isomorphism class if they are isomorphic, but belong to different classes otherwise. For example, the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$ have the same structure and therefore belong to the same isomorphism class, whereas the groups $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$ have structures different from each other and therefore belong to different isomorphism classes.

All the groups in any particular isomorphism class have the same order, since groups of different orders are not isomorphic. You saw earlier that there are only two possible structures for groups of order 4, so there are only two isomorphism classes containing groups of order 4. These are as follows.

- The class of cyclic groups of order 4. Its members include the three groups $(S^+(\square), \circ)$, $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \times_5)$. Each group in this class has exactly two self-inverse elements.
- The class whose members include $(S(\rectangle), \circ)$ and $(U_8, \times_8)$. In each group in this class all four elements are self-inverse.

We use the symbol C_4 to denote a standard, abstract group with the structure of the groups in the first class above, and we refer to it as *the cyclic group of order 4*. We use the symbol V to denote a standard, abstract group with the structure of the groups in the second class above, and we refer to this group as the **Klein four-group**.

The Klein four-group is named after the German mathematician Felix Klein (1849–1925). The symbol V used for the Klein four-group stands for *Vierergruppe*, which was the name given to it by Klein in 1884 in his *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade* (*Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*). It was named for Klein by the Dutch mathematician Bartel van der Waerden (1903–1996) in his *Moderne Algebra* (1930), his influential textbook on abstract algebra. Van der Waerden had studied at the University of Göttingen where Klein had established one of the world's leading mathematics research centres.

Felix Klein

You have seen that there are only two possible structures for groups of order 6, so there are also only two isomorphism classes containing groups of order 6. These are the class containing $(\mathbb{Z}_6, +_6)$ and the class containing $(S(\triangle), \circ)$. We use the symbol C_6 to denote a standard, abstract group with the structure of the groups in the first of these two classes, and we refer to it as *the cyclic group of order 6*. You will learn more about the structure of groups in the second class in Units B3 and B4.

One way to show that two *finite* groups are isomorphic is to rearrange their Cayley tables to have the same pattern, as you saw in the last subsection. Once you have done that, you can obtain an isomorphism from one of the groups to the other by matching up corresponding elements in the rearranged Cayley tables.

For example, at the start of this subsection you saw Cayley tables of the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_5^*, \times_5)$ rearranged to have the same pattern, and a one-to-one correspondence $\phi : S^+(\square) \longrightarrow \mathbb{Z}_5^*$ that matches up corresponding elements in the rearranged Cayley tables. This mapping ϕ is an isomorphism.

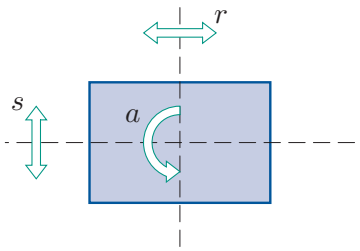


Figure 40 $S(\square)$

Exercise B74

In Exercise B73, near the end of the previous subsection, you should have found the following (though the word 'isomorphic' was not used there).

(a) $(S(\square), \circ)$ is isomorphic to $(U_{12}, \times_{12})$.

(b) $(\mathbb{Z}_4, +_4)$ is isomorphic to $(U_{10}, \times_{10})$.

In each case, by using the solution to Exercise B73, write down an isomorphism from the first group to the second group. (The non-identity elements of $(S(\square), \circ)$ are illustrated in Figure 40 for convenience.)

To show that two *infinite* groups are isomorphic you have to show algebraically that there is an isomorphism from one of the groups to the other, as illustrated in the next worked exercise.

Worked Exercise B29

Let $(G, \times)$ be the cyclic subgroup of the group $(\mathbb{R}, \times)$ generated by the element 2; the set G is given by

$$G = \left\{2^k : k \in \mathbb{Z}\right\}.$$

Prove that $(G, \times)$ is isomorphic to the group $(\mathbb{Z}, +)$ by showing that the following mapping ϕ is an isomorphism:

$$\begin{aligned} \phi\colon G &\longrightarrow \mathbb{Z} \\ 2^k &\longmapsto k. \end{aligned}$$

Solution

By the definition of an isomorphism, we must show that ϕ is one-to-one and onto, and that for all $2^j, 2^k \in G$,

$$\phi(2^j \times 2^k) = \phi(2^j) + \phi(2^k).$$

(The binary operations on the left and right in this equation are those of $(G, \times)$ and $(\mathbb{Z}, +)$, respectively.)

First we check that ϕ is one-to-one. Let $2^j, 2^k \in G$ and suppose that $\phi(2^j) = \phi(2^k)$; that is,

$$j = k.$$

It follows that $2^j = 2^k$. Thus ϕ is one-to-one.

Also, ϕ is onto because each element $k \in \mathbb{Z}$ is the image under ϕ of the element $2^k \in G$.

Finally, for all $2^j, 2^k \in G$,

$$\phi(2^j \times 2^k) = \phi(2^{j+k}) = j + k = \phi(2^j) + \phi(2^k).$$

Thus ϕ is an isomorphism, so $(G, \times) \cong (\mathbb{Z}, +)$.

Notice that in Worked Exercise B29 we took our two arbitrary elements of $(G, \times)$ to be 2^j and 2^k, where $j, k \in \mathbb{Z}$. We could alternatively have taken our two arbitrary elements to be x and y, and then gone on to state that it follows that $x = 2^j$ and $y = 2^k$, where $j, k \in \mathbb{Z}$. However, it is slightly more efficient to take our two elements of $(G, \times)$ to be 2^j and 2^k in the first place. This type of shortcut is sometimes convenient in algebraic arguments, but it is fine to use either approach.

Exercise B75

Prove that the group $(\mathbb{Z}, +)$ is isomorphic to the group $(6\mathbb{Z}, +)$ by showing that the following mapping ϕ is an isomorphism:

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow 6\mathbb{Z} \\ n &\longmapsto 6n. \end{aligned}$$

Once we have built up some knowledge about isomorphism classes of groups, we may be able to use it to help us show that two groups, finite or infinite, are isomorphic. In the next worked exercise this method is used to show that two groups of order 4 are isomorphic.

Worked Exercise B30

Show that the groups $(\{1, -1, i, -i\}, \times)$ (where $i^2 = -1$) and $(\mathbb{Z}_4, +_4)$ are isomorphic.

(You saw that $(\{1, -1, i, -i\}, \times)$ is a group in Exercise B37.)

Solution

Every group of order 4 is isomorphic to either the cyclic group C_4, which has exactly two self-inverse elements, or to the Klein four-group V, which has four self-inverse elements.

In the group $(\{1, -1, i, -i\}, \times)$, which has identity 1, we have

$$1 \times 1 = 1, \quad (-1) \times (-1) = 1, \quad i \times i = -1, \quad (-i) \times (-i) = -1.$$

So exactly two elements are self-inverse and hence this group is isomorphic to C_4.

In the group $(\mathbb{Z}_4, +_4)$, which has identity 0, we have

$$0 +_4 0 = 0, \quad 1 +_4 1 = 2, \quad 2 +_4 2 = 0, \quad 3 +_4 3 = 2.$$

So again exactly two elements are self-inverse and hence this group is isomorphic to C_4.

Since both groups are isomorphic to C_4, they are isomorphic to each other.

Exercise B76

Show that the groups $(U_{12}, \times_{12})$ and $(S(\square), \circ)$ are isomorphic, without using Cayley tables.

The strategy below summarises some methods that you can use for showing that two groups are isomorphic.

Strategy B4

To show that two groups are isomorphic, try one of the following methods.

- Use facts that you know about the structures of the groups (such as whether they are cyclic, or abelian, and how many self-inverse elements they have), together with facts that you know about isomorphism classes.
- If the groups have small finite order, rearrange their Cayley tables to have the same pattern.
- If the groups are infinite or have large finite order, show algebraically that there is an isomorphism from one group to the other.

To help you identify a suitable rearrangement of a Cayley table, or an isomorphism, try using the properties in Theorems B45 and B46 in the next subsection.

Finally in this subsection, here is a comment that you might find interesting, though it is quite complicated and you can skip it if you wish. Isomorphisms provide an explanation of how some groups with unusual binary operations arise. For example, Worked Exercise B18 in Subsection 1.2 involved a group $(X, *)$, where

$$X = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}$$

and $*$ is the binary operation on X defined by

$$(a, b) * (c, d) = (ac, ad + b).$$

This seemingly strange binary operation is revealed as something much more natural if we consider a particular group isomorphic to the group $(X, *)$. It is straightforward to show that the set, A say, of all real functions of the form

$$x \longmapsto ax + b \quad (a, b \in \mathbb{R},\ a \neq 0)$$

forms a group under function composition (it is known as the *one-dimensional affine group over the real numbers*), and that the mapping ϕ from $(A, \circ)$ to $(X, *)$ given by

$$\text{the function } x \longmapsto ax + b \text{ maps to the point } (a, b)$$

is an isomorphism. If we let $f(x) = ax + b$ and $g(x) = cx + d$ be two functions in A, then their composite $f \circ g$ is given by

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f(cx + d) \\ &= a(cx + d) + b \\ &= acx + ad + b,\end{aligned}$$

which demonstrates how the unusual binary operation $*$ of the group $(X, *)$ arises. The point $(ac, ad + b)$ is the image of the function $f \circ g$ above under the isomorphism ϕ.

4.3 Properties of isomorphisms

In this subsection you will meet four theorems that describe some useful properties of isomorphisms and isomorphic groups. These are properties that you would expect to hold simply because isomorphic groups are groups with the same structure, and isomorphisms match up elements that 'have the same role' in that structure. However, formal proofs, using the definition of an isomorphism, are also provided.

Here is the first of these four theorems.

Theorem B45

Let $(G, \circ)$ and $(H, *)$ be groups with identities e_G and e_H, respectively. Any isomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ has the following properties.

(a) ϕ matches the identity elements:

$$\phi(e_G) = e_H.$$

(b) ϕ matches inverses: for each $g \in G$,

$$\phi\left(g^{-1}\right) = (\phi(g))^{-1}.$$

(c) ϕ matches powers of each element: for each $g \in G$ and each $k \in \mathbb{Z}$,

$$\phi\left(g^k\right) = (\phi(g))^k.$$

The properties of isomorphisms in Theorem B45 are illustrated in Figure 41.

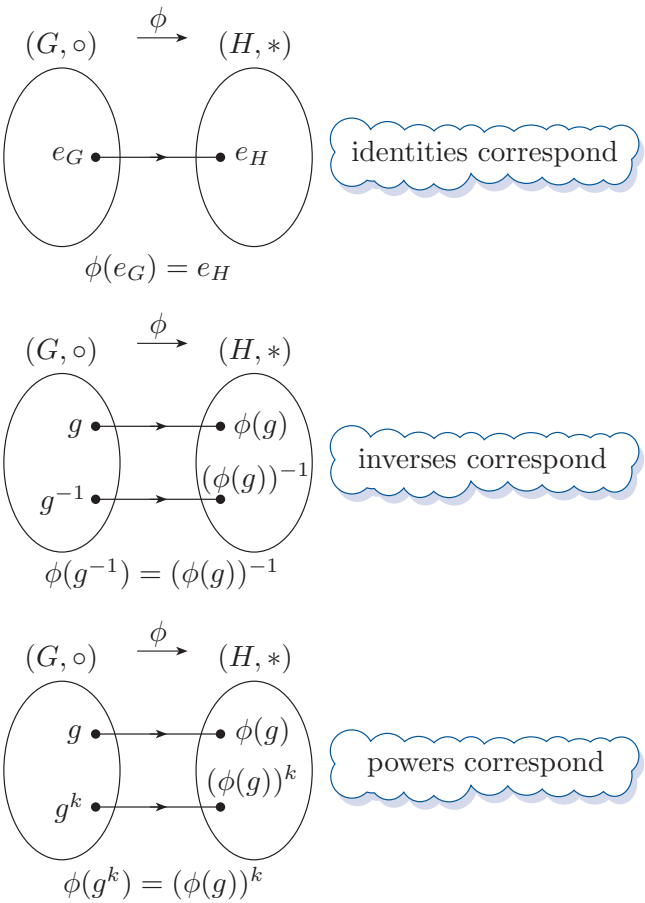


Figure 41 Basic properties of isomorphisms

Proof of Theorem B45

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism.

(a) We have

$$e_G \circ e_G = e_G.$$

Applying the isomorphism ϕ gives

$$\phi(e_G \circ e_G) = \phi(e_G).$$

Since ϕ is an isomorphism, this gives

$$\phi(e_G) * \phi(e_G) = \phi(e_G),$$

and hence

$$\phi(e_G) * \phi(e_G) = \phi(e_G) * e_H.$$

Applying the Left Cancellation Law now gives

$$\phi(e_G) = e_H.$$

(b) Let $g \in G$. Then

$$g \circ g^{-1} = e_G = g^{-1} \circ g.$$

Applying the isomorphism ϕ gives

$$\phi(g \circ g^{-1}) = \phi(e_G) = \phi(g^{-1} \circ g).$$

Since ϕ is an isomorphism and since $\phi(e_G) = e_H$, this gives

$$\phi(g) * \phi(g^{-1}) = e_H = \phi(g^{-1}) * \phi(g).$$

This shows that $\phi(g^{-1})$ is the inverse of $\phi(g)$ in H, that is,

$$\phi(g^{-1}) = (\phi(g))^{-1}.$$

(c) The proof of this property is omitted here as it is quite lengthy, but the next exercise shows that the property is true for $k = 2$, and asks you to deduce that it is true for $k = 3$. Note also that property (b) above is the case $k = -1$. The full proof is included in Book E *Group theory 2*. ■

Exercise B77

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism, and let g be an element of G. Then, since ϕ is an isomorphism,

$$\phi(g \circ g) = \phi(g) * \phi(g),$$

and this equation can be written in terms of powers as

$$\phi(g^2) = (\phi(g))^2, \tag{6}$$

which is Theorem B45(c) in the case $k = 2$.

By writing $g^3 = g^2 \circ g$ and using the fact that ϕ is an isomorphism, together with equation (6), prove that

$$\phi(g^3) = (\phi(g))^3.$$

As usual with results in group theory, Theorem B45 is stated in multiplicative notation, but you need to be able to apply it to additive groups as well as to multiplicative groups. For example, property (c) in the theorem, with $k = 3$, tells you that if $(G, \times)$ and $(H, +)$ are groups and $\phi : (G, \times) \longrightarrow (H, +)$ is an isomorphism, then for any element $g \in G$ we have

$$\phi(g^3) = 3\phi(g)$$

(which we can also write as

$$\phi(g \times g \times g) = \phi(g) + \phi(g) + \phi(g).)$$

The next theorem gives some further useful properties of isomorphisms.

Theorem B46

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism. Let $g \in G$.

- If g has order n, then so does $\phi(g)$.
- If g has infinite order, then so does $\phi(g)$.

Proof Let the identities of $(G, \circ)$ and $(H, *)$ be e_G and e_H, respectively. For any $k \in \mathbb{N}$, the equation

$$g^k = e_G$$

is equivalent to the equation

$$\phi(g^k) = \phi(e_G),$$

(since ϕ is a one-to-one mapping), and this equation is in turn equivalent to the equation

$$(\phi(g))^k = e_H$$

(by properties (a) and (c) in Theorem B45).

Hence the set of integers k for which $g^k = e_G$ is exactly the same as the set of integers k for which $(\phi(g))^k = e_H$. The two statements in the theorem follow immediately. ■

The third theorem in this subsection tells us that, as you would expect, isomorphisms match up subgroups. For example, consider the isomorphic groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_5, \times_5)$, and the following isomorphism between them, which you met in Subsection 4.2:

$$\begin{aligned} \phi : S^+(\square) &\longrightarrow \mathbb{Z}_5^* \\ e &\longmapsto 1 \\ a &\longmapsto 2 \\ b &\longmapsto 4 \\ c &\longmapsto 3, \end{aligned}$$

We know that $K = \{e, b\}$ is a subgroup of $(S^+(\square), \circ)$ (it is the cyclic subgroup generated by b). Correspondingly, the image of this subgroup under ϕ, which is

$$\phi(K) = \{\phi(k) : k \in K\} = \{\phi(e), \phi(b)\} = \{1, 4\},$$

is a subgroup of $(\mathbb{Z}_5, \times_5)$. Here is the general result.

Theorem B47

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism. If K is a subgroup of $(G, \circ)$, then

$$\phi(K) = \{\phi(k) : k \in K\}$$

is a subgroup of $(H, *)$.

Proof Certainly $\phi(K)$ is a subset of H. We show that $(\phi(K), *)$ is a subgroup of $(H, *)$ by showing that it satisfies the three subgroup properties.

SG1 Closure

Let $l_1, l_2 \in \phi(K)$; then $l_1 = \phi(k_1)$ and $l_2 = \phi(k_2)$ for some $k_1, k_2 \in K$. Hence

$$\begin{aligned} l_1 * l_2 &= \phi(k_1) * \phi(k_2) \\ &= \phi(k_1 \circ k_2) \quad \text{(since } \phi \text{ is an isomorphism).} \end{aligned}$$

Now $k_1 \circ k_2 \in K$, because K is a subgroup of $(G, \circ)$, so this shows that $l_1 * l_2 \in \phi(K)$. Thus $\phi(K)$ is closed under $*$.

SG2 Identity

Let e_G and e_H be the identities of $(G, \circ)$ and $(H, *)$, respectively. Then $\phi(e_G) = e_H$, by Theorem B45(a). Now $e_G \in K$, because K is a subgroup of $(G, \circ)$, so this shows that $e_H \in \phi(K)$.

SG3 Inverses

Let $l \in \phi(K)$; then $l = \phi(k)$ for some $k \in K$. Hence

$$\begin{aligned} l^{-1} &= (\phi(k))^{-1} \\ &= \phi(k^{-1}) \quad \text{(by Theorem B45(b)).} \end{aligned}$$

Now $k^{-1} \in K$, because K is a subgroup of $(G, \circ)$, so this shows that $l^{-1} \in \phi(K)$. Thus $\phi(K)$ contains the inverse of each of its elements.

Hence $(\phi(K), *)$ satisfies the three subgroup properties, and so is a subgroup of $(H, *)$. ■

The final theorem in this subsection states some properties of isomorphic groups. As with the earlier properties, you would expect these properties to hold, simply because saying that two groups are isomorphic means that they have the same structure. However, formal proofs are provided.

Theorem B48

Let $(G, \circ)$ and $(H, *)$ be isomorphic groups.

(a) If $(G, \circ)$ is abelian then so is $(H, *)$.

(b) If $(G, \circ)$ is cyclic then so is $(H, *)$.

Proof Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism.

(a) Suppose that $(G, \circ)$ is abelian. We have to show that $(H, *)$ is abelian. Let h_1, h_2 be any elements of H. Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. Since $(G, \circ)$ is abelian, we have

$$g_1 \circ g_2 = g_2 \circ g_1.$$

Hence

$$\phi(g_1 \circ g_2) = \phi(g_2 \circ g_1).$$

Since ϕ is an isomorphism, this gives

$$\phi(g_1) * \phi(g_2) = \phi(g_2) * \phi(g_1),$$

that is,

$$h_1 * h_2 = h_2 * h_1.$$

This shows that $(H, *)$ is abelian.

(b) Suppose that $(G, \circ)$ is cyclic, generated by a. We will show that $(H, *)$ is also cyclic, generated by $\phi(a)$. Let h be any element of H. We have to show that h can be expressed as a power of $\phi(a)$. Now $h = \phi(g)$ for some $g \in G$. Since $(G, \circ)$ is generated by a, we have

$$g = a^k$$

for some integer k. Hence

$$\phi(g) = \phi(a^k).$$

By Theorem B45(c), this gives

$$\phi(g) = (\phi(a))^k,$$

that is,

$$h = (\phi(a))^k.$$

This expresses h as a power of $\phi(a)$. Thus $(H, *)$ is cyclic, generated by $\phi(a)$. ■

You can sometimes use some of the properties of isomorphisms and isomorphic groups that you have met in this subsection and in the previous subsection to show that two particular groups are *not* isomorphic. Unfortunately there is no general, systematic procedure for showing that two groups are not isomorphic: you just have to find some means of demonstrating that they have different structures. Some suggestions are given in the strategy below.

Strategy B5

To show that two groups are not isomorphic, try any of the following methods.

- Compare their orders: if one group is finite and the other is infinite, or if they have different finite orders, then they are not isomorphic.
- Ascertain whether they are abelian or cyclic: if one group is abelian and the other is not, or if one group is cyclic and the other is not, then they are not isomorphic.
- Compare the numbers of self-inverse elements: if one group has more self-inverse elements than the other, then they are not isomorphic.
- Compare the entries in the main diagonals of their Cayley tables, if these are available. For example, count the numbers of different elements that appear: if the count is different for the two groups, then they are not isomorphic.
- Compare the numbers of elements of a particular order: if one group has more elements of this order than the other, then they are not isomorphic.

The fourth suggestion in the box above relies on the fact that the n elements (not necessarily distinct) that occur on the main diagonal of the Cayley table of a group of order n are the n elements obtained by composing each group element with itself. So rearranging the borders of the Cayley table will not change these n elements, though it may change their positions on the diagonal.

Exercise B78

In each of the following cases, show that the two groups are not isomorphic.

(a) $(\mathbb{Z}_8, +_8)$ and $(S(\triangle), \circ)$.

(b) $(\mathbb{Z}_8, +_8)$ and $(U_{20}, \times_{20})$.

(You were asked to investigate some properties of the group $(U_{20}, \times_{20})$ in Exercise B65.)

4.4 Isomorphisms of cyclic groups

Near the end of Subsection 3.4 you saw that the groups $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$ have the same structure, namely a cyclic structure, as shown in Figure 42.

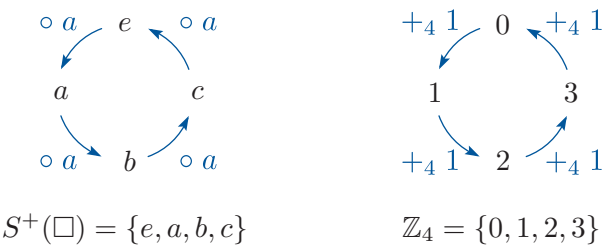


Figure 42 The cycle of powers of a in $(S^+(\square), \circ)$ and the cycle of multiples of 1 in $(\mathbb{Z}_4, +_4)$

Each power of the generator a in $(S^+(\square), \circ)$ matches up with the corresponding multiple of the generator 1 in the additive group $(\mathbb{Z}_4, +_4)$ to give the following isomorphism:

$$\begin{aligned}\phi : S^+(\square) &\longrightarrow \mathbb{Z}_4\\ e = a^0 &\longmapsto 0 \times 1 = 0\\ a = a^1 &\longmapsto 1 \times 1 = 1\\ b = a^2 &\longmapsto 2 \times 1 = 2\\ c = a^3 &\longmapsto 3 \times 1 = 3.\end{aligned}$$

This isomorphism is set out again below, with the powers in $(S^+(\square), \circ)$ and the multiples in $(\mathbb{Z}_4, +_4)$ expanded to make it clear how the elements match up:

$$\begin{aligned}\phi : S^+(\square) &\longrightarrow \mathbb{Z}_4\\ e &\longmapsto 0\\ a &\longmapsto 1\\ a \circ a &\longmapsto 1 +_4 1\\ a \circ a \circ a &\longmapsto 1 +_4 1 +_4 1.\end{aligned}$$

More generally, consider any two finite cyclic groups $(G, \circ)$ and $(H, *)$ with the same order n. They have the same structure, as shown in Figure 43; here a and b are generators of $(G, \circ)$ and $(H, *)$, respectively.

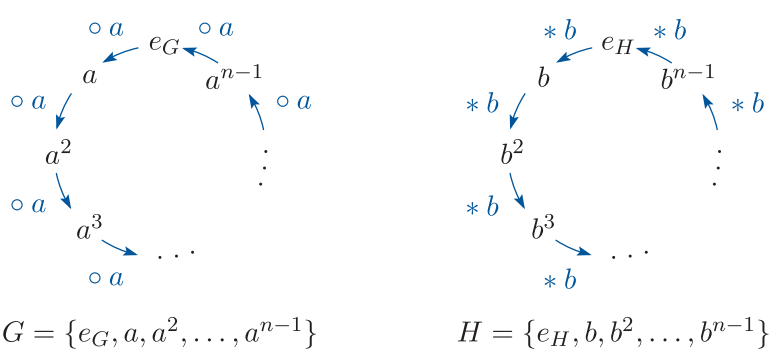


Figure 43 The cycles of powers of a generator in two cyclic groups of order n

Each power of the generator a of the first cyclic group matches up with the corresponding power of the generator b of the second group, to give the isomorphism

$$\begin{aligned}\phi : G &\longrightarrow H\\ e_G &\longmapsto e_H\\ a &\longmapsto b\\ a^2 &\longmapsto b^2\\ a^3 &\longmapsto b^3\\ &\vdots\\ a^{n-1} &\longmapsto b^{n-1}.\end{aligned}$$

This isomorphism can be written more concisely as

$$\begin{aligned}\phi : G &\longrightarrow H\\ a^k &\longmapsto b^k \quad (k = 0, 1, \ldots, n-1).\end{aligned}$$

That is, we have the theorem below.

Theorem B49

Let $(G, \circ)$ and $(H, *)$ be finite cyclic groups of the same order n, generated by a and b, respectively. Then $(G, \circ)$ and $(H, *)$ are isomorphic, and an isomorphism is given by

$$\begin{aligned}\phi : G &\longrightarrow H\\ a^k &\longmapsto b^k \quad (k = 0, 1, \ldots, n-1).\end{aligned}$$

Proof The mapping ϕ defined above is one-to-one and onto. Also, for all $a^j, a^k \in G$,

$$\phi(a^j \circ a^k) = \phi(a^{j+k}) = b^{j+k} = b^j * b^k = \phi(a^j) * \phi(a^k).$$

So ϕ is an isomorphism. ■

Since all cyclic groups of any particular order are isomorphic to each other, the notation below is sometimes useful. You have met this notation already for cyclic groups of orders 4 and 6.

Notation

The notation C_n denotes a standard, abstract cyclic group of order n. We refer to it as *the cyclic group of order n*.

Theorem B49 gives us the following strategy for finding an isomorphism from one finite cyclic group to another of the same order.

Strategy B6

To find an isomorphism between two finite cyclic groups $(G, \circ)$ and $(H, *)$ of the same order n, do the following.

1. Find a generator a of $(G, \circ)$ and a generator b of $(H, *)$.
2. Construct the isomorphism

$$\begin{aligned} \phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k = 0, 1, \ldots, n-1). \end{aligned}$$

Keep in mind that if you want to apply Strategy B6 to two groups where either or both are *additive* cyclic groups, then you need to translate step 2 of the strategy into additive notation as appropriate. For an additive cyclic group $(G, +)$ generated by a, the power a^k becomes the multiple ka, and similarly for an additive cyclic group $(H, +)$ generated by b, the power b^k becomes the multiple kb.

You have seen that usually a cyclic group has more than one generator. By applying Strategy B6 more than once, using different generators, we can find more than one isomorphism between two finite cyclic groups of the same order.

Worked Exercise B31

Find two isomorphisms from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$.

Solution

Use Strategy B6. To find one isomorphism, first find a generator of each group. Match up corresponding powers of the generators, starting by matching the identities of each group (the zeroth powers).

The group $(\mathbb{Z}_4, +_4)$ is generated by 1; the group $(\mathbb{Z}_5^*, \times_5)$ is generated by 2 (as found in Exercise B58(c)). So an isomorphism is given by

$$\begin{aligned} \phi : \mathbb{Z}_4 &\longrightarrow \mathbb{Z}_5^* \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 2 \\ 1 +_4 1 &\longmapsto 2 \times_5 2 \\ 1 +_4 1 +_4 1 &\longmapsto 2 \times_5 2 \times_5 2, \end{aligned}$$

that is,

$$\begin{aligned} \phi : \mathbb{Z}_4 &\longrightarrow \mathbb{Z}_5^* \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 2 \\ 2 &\longmapsto 4 \\ 3 &\longmapsto 3. \end{aligned}$$

To find a different isomorphism, find a different generator of one of the groups.

The group $(\mathbb{Z}_4, +_4)$ is also generated by 3, so another isomorphism is given by

$$\begin{aligned} \phi : \mathbb{Z}_4 &\longrightarrow \mathbb{Z}_5^* \\ 0 &\longmapsto 1 \\ 3 &\longmapsto 2 \\ 3 +_4 3 &\longmapsto 2 \times_5 2 \\ 3 +_4 3 +_4 3 &\longmapsto 2 \times_5 2 \times_5 2, \end{aligned}$$

that is,

$$\begin{aligned} \phi : \mathbb{Z}_4 &\longrightarrow \mathbb{Z}_5^* \\ 0 &\longmapsto 1 \\ 3 &\longmapsto 2 \\ 2 &\longmapsto 4 \\ 1 &\longmapsto 3. \end{aligned}$$

Exercise B79

(a) Write down the elements of the set U_9 of integers in $\mathbb{Z}_9$ coprime to 9. Show that the group $(U_9, \times_9)$ is cyclic and find all its generators.

(b) Hence find two isomorphisms $\phi : (U_9, \times_9) \longrightarrow (\mathbb{Z}_6, +_6)$.

Exercise B80

(a) Let $G = \{1, 2, 4, 8, 9, 13, 15, 16\}$. Show that $(G, \times_{17})$ is a cyclic group, and find all its generators.

(b) Let $(C, \circ)$ be an abstract cyclic group of order 8, generated by the element x, so that

$$C = \{e, x, x^2, x^3, x^4, x^5, x^6, x^7\}.$$

Find four isomorphisms $\phi : (G, \times_{17}) \longrightarrow (C, \circ)$.

Theorem B49 tells us in particular that every cyclic group of order n is isomorphic to the cyclic group $(\mathbb{Z}_n, +_n)$. Hence the results about $(\mathbb{Z}_n, +_n)$ that you met in Subsection 3.4 provide results about *every* cyclic group of order n. For example, you saw in Theorem B41 in Subsection 3.4 that the group $(\mathbb{Z}_n, +_n)$ has exactly one cyclic subgroup of order q for each positive factor q of n, and no other subgroups. By Theorem B49 (and Theorem B47), the same is true of *every* cyclic group of order n.

Powers of generators in infinite cyclic groups can be matched up in the same way as those in finite cyclic groups, which gives the following theorem.

Theorem B50

Let $(G, \circ)$ and $(H, *)$ be infinite cyclic groups, generated by a and b, respectively. Then $(G, \circ)$ and $(H, *)$ are isomorphic, and an isomorphism is given by

$$\begin{aligned} \phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k \in \mathbb{Z}). \end{aligned}$$

Proof The proof of Theorem B49 applies here also. ■

The idea of isomorphism is extremely important in group theory. As you saw above, it allows us to prove results about the structure of one group, or one family of groups, and know that these results also apply to many other groups – namely, to all groups isomorphic to the group or groups that we considered.

Summary

In this unit you studied the structures of groups. You saw that groups can have *subgroups*, and looked at some ways in which subgroups of a group can be found. You saw that the set consisting of all the powers of an element of a group is always a subgroup of the group, called the *cyclic subgroup generated* by that element. You met the idea of a *cyclic* group, which is a group that itself consists of all the powers of one of its elements, and you studied some properties of cyclic groups. You learned about the different notations used for additive and multiplicative groups. Finally, you met the powerful concept of *isomorphism*, which links groups that have the same structure and which can therefore be considered in a sense to be 'the same group'.

Learning outcomes

After working through this unit, you should be able to:

- understand what is meant by a *subgroup*
- use the three subgroup properties to determine whether $(H, \circ)$ is a subgroup of a group $(G, \circ)$, where H is a subset of the set G
- find subgroups of a symmetry group $S(F)$ by adding features to the figure F, or by fixing a feature of F
- translate results in group theory from multiplicative notation to additive notation, and vice versa
- understand what is meant by the *order* of a group element and the *cyclic subgroup generated* by a group element, and find these for group elements of reasonably small order
- understand the terms *cyclic group*, and *generator* of a cyclic group
- know that every subgroup of a cyclic group is also cyclic
- find all the subgroups and all the generators of a cyclic group of any reasonably small order, and in particular do this efficiently for $(\mathbb{Z}_n, +_n)$
- explain the meaning of the terms *isomorphic groups* and *isomorphism*
- in some cases, show that two groups are isomorphic and find an isomorphism, or show that the groups are not isomorphic
- know that any two cyclic groups of the same order are isomorphic, and find isomorphisms from one cyclic group to another of the same order
- know some basic properties of isomorphisms and isomorphic groups.

Solutions to exercises

Solution to Exercise B35

(a) We obtain a Cayley table for $\{e, s\}$ under $\circ$ by deleting the rows and columns labelled a, b, r and t in the group table of $(S(\triangle), \circ)$:

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$\longrightarrow$

$\circ$	e	s
e	e	s
s	s	e

We now check the four group axioms.

G1 Every element in the body of the table is in the set $\{e, s\}$, so $\{e, s\}$ is closed under function composition.

G2 Function composition is associative.

G3 The row and column labelled e repeat the table borders, so e is an identity element.

G4 We see that e and s are both self-inverse.

Hence $(\{e, s\}, \circ)$ satisfies the four group axioms, and so is a group.

The set $\{e, s\}$ is a subset of the set $S(\triangle)$, so $(\{e, s\}, \circ)$ is a subgroup of $(S(\triangle), \circ)$.

(b) We obtain a Cayley table for $\{e, b, r\}$ under $\circ$ by deleting the rows and columns labelled by a, s and t in the group table of $(S(\triangle), \circ)$:

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$\longrightarrow$

$\circ$	e	b	r
e	e	b	r
b	b	a	s
r	r	t	e

We now check the group axioms.

G1 The Cayley table for $\{e, b, r\}$ contains elements other than e, b and r, so $\{e, b, r\}$ is not closed under the operation $\circ$. That is, axiom G1 fails.

Hence $(\{e, b, r\}, \circ)$ is not a group, and therefore it is not a subgroup of $(S(\triangle), \circ)$.

Solution to Exercise B36

We have $\{e, b, s, u\} \subseteq S(\square)$, and the binary operation $\circ$ is the same on each set.

The Cayley table for $(\{e, b, s, u\}, \circ)$ is as follows.

$\circ$	e	b	s	u
e	e	b	s	u
b	b	e	u	s
s	s	u	e	b
u	u	s	b	e

We check the three subgroup properties.

SG1 Every element in the body of the table is in $\{e, b, s, u\}$, so this set is closed under function composition.

SG2 The identity element in $S(\square)$ is e, and we have $e \in \{e, b, s, u\}$.

SG3 The elements e, b, s and u are all self-inverse, so $\{e, b, s, u\}$ contains the inverse of each of its elements.

Hence $(\{e, b, s, u\}, \circ)$ satisfies the three subgroup properties, and so is a subgroup of $(S(\square), \circ)$.

Solution to Exercise B37

(a) The Cayley table for $(\{1, -1, i, -i\}, \times)$ is as follows.

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(b) We have $\{1, -1, i, -i\} \subseteq \mathbb{C}^*$, and the binary operation $\times$ is the same on each set.

We check the three subgroup properties.

SG1 Every element in the body of the table is in $\{1, -1, i, -i\}$, so this set is closed under multiplication.

SG2 The identity element in $\mathbb{C}^*$ is 1, and $1 \in \{1, -1, i, -i\}$.

SG3 From the table, we see that the elements 1 and -1 are self-inverse, and i and $-i$ are inverses of each other, so $\{1, -1, i, -i\}$ contains the inverse of each of its elements.

Hence $(\{1, -1, i, -i\}, \times)$ satisfies the three subgroup properties, and so is a subgroup of $(\mathbb{C}^*, \times)$.

(The easiest way to find the inverses of i and $-i$ here is to use the Cayley table, but you could also just use arithmetic in $\mathbb{C}$ in the usual way. For example, the multiplicative inverse of i is

$$\frac{1}{i} = \frac{1 \times (-i)}{i \times (-i)} = \frac{-i}{1} = -i.)$$

Solution to Exercise B38

We have $3\mathbb{Z} \subseteq \mathbb{Z}$, and the binary operation $+$ is the same on each set.

We show that the three subgroup properties hold.

SG1 Let $x, y \in 3\mathbb{Z}$; then $x = 3r$ and $y = 3s$, for some $r, s \in \mathbb{Z}$. Thus

$$x + y = 3r + 3s = 3(r + s).$$

Since $r + s$ is an integer, it follows that $x + y \in 3\mathbb{Z}$. Hence $3\mathbb{Z}$ is closed under addition.

SG2 The identity in $(\mathbb{Z}, +)$ is 0, and $0 = 3 \times 0 \in 3\mathbb{Z}$, so $3\mathbb{Z}$ contains the identity.

SG3 Let $x \in 3\mathbb{Z}$. Then $x = 3r$ for some $r \in \mathbb{Z}$. The inverse of $x = 3r$ in $(\mathbb{Z}, +)$ is

$$-x = -3r = 3(-r),$$

which is an element of $3\mathbb{Z}$ since $-r$ is an integer. Thus $3\mathbb{Z}$ contains the inverse of each of its elements.

Hence $(3\mathbb{Z}, +)$ satisfies the three subgroup properties, and so is a subgroup of $(\mathbb{Z}, +)$.

Solution to Exercise B39

(a) $(6\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$, by the result in the box immediately before the exercise.

(b) By the result in the box, both $(6\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are groups. Also, $6\mathbb{Z} \subseteq 2\mathbb{Z}$, since every multiple of 6 is also a multiple of 2. So $(6\mathbb{Z}, +)$ is a subgroup of $(2\mathbb{Z}, +)$.

(Notice that there is no need to check the three subgroup properties here, because we already know that both $(6\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are groups, by the result in the box.)

(c) $5\mathbb{Z}$ is not a subset of $3\mathbb{Z}$; for example, 5 is a multiple of 5 but is not a multiple of 3. Hence $(5\mathbb{Z}, +)$ is not a subgroup of $(3\mathbb{Z}, +)$.

Solution to Exercise B40

(a) The set $\mathbb{Q}^*$ is not a subset of $\mathbb{R}^+$; for example, $-1 \in \mathbb{Q}^*$, but $-1 \notin \mathbb{R}^+$, so $\mathbb{Q}^* \not\subseteq \mathbb{R}^+$. It follows that $(\mathbb{Q}^*, \times)$ is not a subgroup of $(\mathbb{R}^+, \times)$.

(b) We have $W \subseteq \mathbb{Z}$, and the binary operation is the same on each set.

However, we have $1 \in W$, but the inverse of 1 in $(\mathbb{Z}, +)$, namely -1, is not in W. So property SG3 fails and hence $(W, +)$ is not a subgroup of $(\mathbb{Z}, +)$.

Solution to Exercise B41

We have $H \subseteq \mathbb{Z}_{12}$, and the binary operation $+_{12}$ is the same on each set.

We show that the three subgroup properties hold.

The Cayley table for $(H, +_{12})$ is as follows.

$+_{12}$	0	3	6	9
0	0	3	6	9
3	3	6	9	0
6	6	9	0	3
9	9	0	3	6

SG1 Every element in the table is in H, so H is closed under $+_{12}$.

SG2 The identity in $(\mathbb{Z}_{12}, +_{12})$ is 0, and $0 \in H$.

SG3 From the Cayley table, we see that the inverse of each element of H is in H, as below.

Element	0	3	6	9
Inverse	0	9	6	3

Hence $(H, +_{12})$ satisfies the three subgroup properties, and so is a subgroup of $(\mathbb{Z}_{12}, +_{12})$.

Solution to Exercise B42

(a) Property SG1 fails: $a \circ a = b$, but $b \notin H$.

(b) Property SG1 fails: $2 \times_5 3 = 1$, but $1 \notin H$.

(Alternatively, property SG2 fails: the identity in $\mathbb{Z}_5^*$ is 1, but $1 \notin H$.)

(c) Property SG3 fails: for example, the inverse of 2 in $(\mathbb{R}^*, \times)$ is $\frac{1}{2}$, but $\frac{1}{2} \notin \mathbb{Z}^*$.

Solution to Exercise B43

(a) We show that $(X, *)$ satisfies the four group axioms.

G1 Let $(a, b), (c, d) \in X$; then $a \neq 0$, $b \neq 0$, $c \neq 0$ and $d \neq 0$. We have

$$(a, b) * (c, d) = (ac, bd).$$

This point is in $\mathbb{R}^2$ since $a, b, c, d \in \mathbb{R}$. Also $ac \neq 0$ because $a \neq 0$ and $c \neq 0$, and similarly $bd \neq 0$ because $b \neq 0$ and $d \neq 0$. So this point is in X. Thus X is closed under $*$.

G2 Let $(a, b), (c, d), (e, f) \in X$. We have

$$\begin{aligned}&(a, b) * ((c, d) * (e, f))\\ &= (a, b) * (ce, df)\\ &= (ace, bdf),\end{aligned}$$

and

$$\begin{aligned}&((a, b) * (c, d)) * (e, f)\\ &= (ac, bd) * (e, f)\\ &= (ace, bdf).\end{aligned}$$

The two expressions obtained are the same, so $*$ is associative on X.

G3 Suppose that (x, y) is an identity in X. Then we must have, for each $(a, b) \in X$,

$$(a, b) * (x, y) = (a, b) = (x, y) * (a, b).$$

The left-hand equation gives

$$(ax, by) = (a, b).$$

Comparing coordinates, we obtain

$$ax = a \quad \text{and} \quad by = b.$$

Since these equations must hold for all non-zero values of a and b, we must have

$$x = y = 1.$$

So the only possibility for an identity is $(1, 1)$.

Now $(1, 1)$ is in X, since it is in $\mathbb{R}^2$ and both its coordinates are non-zero, and for all $(a, b) \in X$, we have

$$(a, b) * (1, 1) = (a, b),$$

and

$$(1, 1) * (a, b) = (a, b).$$

So $(1, 1)$ is an identity for $*$ on X.

G4 Let $(a, b) \in X$; then $a \neq 0$ and $b \neq 0$. Suppose that (x, y) is an inverse of (a, b). Then we must have

$$(a, b) * (x, y) = (1, 1) = (x, y) * (a, b).$$

The left-hand equation gives

$$(ax, by) = (1, 1).$$

Comparing coordinates, we obtain

$$ax = 1 \quad \text{and} \quad by = 1.$$

Since $a \neq 0$ and $b \neq 0$, these equations give

$$x = 1/a \quad \text{and} \quad y = 1/b.$$

So the only possibility for an inverse of (a, b) is $(1/a, 1/b)$.

Now $(1/a, 1/b) \in X$, since both its coordinates are non-zero, and we have

$$(a, b) * (1/a, 1/b) = (1, 1),$$

and

$$(1/a, 1/b) * (a, b) = (1, 1).$$

So $(1/a, 1/b)$ is an inverse of (a, b). Thus every element of X has an inverse in X.

Hence $(X, *)$ satisfies the four group axioms, and so is a group.

(b) (i) We can simplify the description of the set A, as follows:

$$A = \{(a, b) \in X : a = 1\} = \{(1, b) : b \in \mathbb{R}^*\}.$$

We show that $(A, *)$ satisfies the three subgroup properties.

SG1 Let $(1, b), (1, d) \in A$; then $b \neq 0$ and $d \neq 0$. We have

$$(1, b) * (1, d) = (1, bd).$$

This point is in A because its first coordinate is 1 and its second coordinate is non-zero, since $b \neq 0$ and $d \neq 0$. Thus A is closed under $*$.

SG2 The identity in X is $(1, 1)$. This point is in A, because its first coordinate is 1 and its second coordinate is non-zero.

SG3 Let $(1, b) \in A$. By the solution to part (a), the inverse of $(1, b)$ in A is $(1/1, 1/b) = (1, 1/b)$. This point has first coordinate 1 and its second coordinate is non-zero, so it is in A. Thus A contains the inverse of each of its elements.

Hence $(A, *)$ satisfies the three subgroup properties, and so is a subgroup of $(X, *)$.

(ii) The points $(3, -1)$ and $(4, -2)$ are in B, but

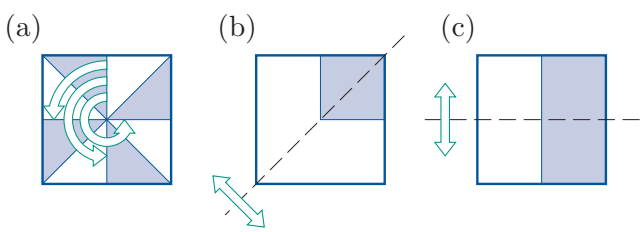
$$(3, -1) * (4, -2) = (12, 2) \notin B.$$

Thus B is not closed under $*$; that is, property SG1 fails.

Hence $(B, *)$ is not a subgroup of $(X, *)$.

Solution to Exercise B44

The non-identity symmetries of the three modified squares are shown below.



(a) The symmetry group of the modified square is

$$\{e, a, b, c\} = S^+(\square).$$

(Any reflection interchanges the shaded and unshaded areas.)

(b) The symmetry group of the modified square is

$$\{e, u\}.$$

(The other elements of $S(\square)$ move the shaded square to a different corner.)

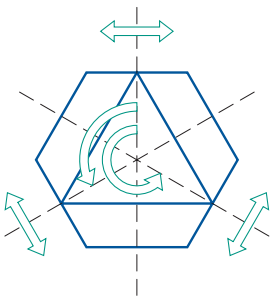
(c) The symmetry group of the modified square is

$$\{e, t\}.$$

(The other elements of $S(\square)$ move the shaded rectangle to other parts of the square.)

Solution to Exercise B45

The non-identity symmetries of F' are shown below.



The elements of $S(F')$ are:

- the identity
- rotations through $2\pi/3$ and $4\pi/3$ about the centre
- reflections in the three axes shown above.

The other elements of $S(\hexagon)$ do not map the triangle to itself. Thus the effect of the inscribed equilateral triangle is to restrict the symmetries of the modified hexagon to those of the triangle.

Solution to Exercise B46

The required subgroup is

$$\left\{ \begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 2&4&3&1 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 4&1&3&2 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 2&1&3&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 4&2&3&1 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 1&4&3&2 \end{pmatrix} \right\}.$$

(One way to obtain these two-line symbols is to start with the subgroup in Worked Exercise B21, replace each occurrence of the symbol 3 with the symbol 4 and vice versa, and then rearrange the columns in each two-line symbol so that the numbers in the top row are in the natural order.)

Solution to Exercise B47

The required subgroup is

$$\left\{ \begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 1&2&4&3 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 2&1&3&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 2&1&4&3 \end{pmatrix} \right\}.$$

(It consists of all the elements of $S(\text{tet})$ that either fix the vertices at locations 1 and 2, or interchange them.)

Solution to Exercise B48

(a) The symmetries of the modified framework prism form a subgroup of $S(F)$ whose elements are as follows.

The identity:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

The rotation through π about the vertical axis through the centre of the prism:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

The reflection in the vertical plane through locations 1 and 4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix}.$$

The reflection in the vertical plane through the midpoints of the edges joining the vertices at locations 1 and 4, 2 and 5, and 3 and 6:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}.$$

Thus we obtain a subgroup of $S(F)$ of order 4 (that is, with 4 elements).

(b) Here, the symmetries of the modified framework prism are 'essentially the same' as those of $S(\triangle)$, so we obtain a subgroup of $S(F)$ whose elements are as follows.

The identity:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

The rotations through $2\pi/3$ and $4\pi/3$ about the horizontal axis of symmetry:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix}.$$

The reflection in the vertical plane through locations 1 and 4, and the midpoints of the edges joining the vertices at locations 2 and 3, and 5 and 6:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix}.$$

The reflection in the plane through locations 2 and 5, and the midpoints of the edges joining the vertices at locations 1 and 3, and 4 and 6:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}.$$

The reflection in the plane through locations 3 and 6, and the midpoints of the edges joining the vertices at locations 1 and 2, and 4 and 5:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{pmatrix}.$$

Thus we obtain a subgroup of $S(F)$ of order 6.

(c) The symmetries of the modified framework prism, with the vertices at locations 1 and 4 fixed, form a subgroup of $S(F)$ whose elements are as follows.

The identity:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

The reflection in the plane through locations 1 and 4, and the midpoints of the edges joining the vertices at locations 2 and 3, and 5 and 6:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix}.$$

Thus we obtain a subgroup of $S(F)$ of order 2.

Solution to Exercise B49

(a) $a^0 = e,$

$a^1 = a,$

$a^2 = a \circ a$
$\quad = b,$

$a^3 = a \circ a \circ a$
$\quad = b \circ a$
$\quad = c,$

$a^4 = a \circ a \circ a \circ a$
$\quad = c \circ a$
$\quad = e,$

$a^5 = a \circ a \circ a \circ a \circ a$
$\quad = e \circ a$
$\quad = a.$

(b) $a^{-1} = c$,

$$\begin{aligned} a^{-2} &= a^{-1} \circ a^{-1} \\ &= c \circ c \\ &= b, \\ a^{-3} &= a^{-1} \circ a^{-1} \circ a^{-1} \\ &= b \circ c \\ &= a, \\ a^{-4} &= a^{-1} \circ a^{-1} \circ a^{-1} \circ a^{-1} \\ &= a \circ c \\ &= e, \\ a^{-5} &= a^{-1} \circ a^{-1} \circ a^{-1} \circ a^{-1} \circ a^{-1} \\ &= e \circ c \\ &= c. \end{aligned}$$

(c) $b^0 = e$,

$$\begin{aligned} b^1 &= b, \\ b^2 &= b \circ b \\ &= e, \\ b^3 &= b \circ b \circ b \\ &= e \circ b \\ &= b \\ b^4 &= b \circ b \circ b \circ b \\ &= b \circ b \\ &= e. \end{aligned}$$

(d) $b^{-1} = b$,

$$\begin{aligned} b^{-2} &= b^{-1} \circ b^{-1} \\ &= b \circ b \\ &= e, \\ b^{-3} &= b^{-1} \circ b^{-1} \circ b^{-1} \\ &= e \circ b \\ &= b. \end{aligned}$$

(e) $r^0 = e$,

$$\begin{aligned} r^1 &= r, \\ r^2 &= r \circ r \\ &= e, \\ r^3 &= r \circ r \circ r \\ &= e \circ r \\ &= r \\ r^4 &= r \circ r \circ r \circ r \\ &= r \circ r \\ &= e. \end{aligned}$$

Solution to Exercise B50

We have

$$\begin{aligned} x^2 \circ (x^{-1})^2 &= x \circ x \circ x^{-1} \circ x^{-1} \\ &= x \circ e \circ x^{-1} \\ &= x \circ x^{-1} \\ &= e, \end{aligned}$$

and similarly,

$$\begin{aligned} (x^{-1})^2 \circ x^2 &= x^{-1} \circ x^{-1} \circ x \circ x \\ &= x^{-1} \circ e \circ x \\ &= x^{-1} \circ x \\ &= e. \end{aligned}$$

Thus $(x^{-1})^2$ is an inverse of x^2, and, since the inverse of any group element is unique, it follows that $(x^{-1})^2$ is the inverse of x^2.

Solution to Exercise B51

(a) $x^0 = e$ translates to

$$0x = 0.$$

(b) $x \circ x^{-1} = e$ translates to

$$x + (-x) = 0.$$

(c) $x \circ x^2 = x^3$ translates to

$$x + 2x = 3x.$$

(d) $(x^{-1})^{-1} = x$ translates to

$$-(-x) = x.$$

(e) $e \circ x = x$ translates to

$$0 + x = x.$$

(f) $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$ translates to

$$-(x + y) = (-y) + (-x),$$

or alternatively, since $(G, +)$ is abelian,

$$-(x + y) = (-x) + (-y).$$

Solution to Exercise B52

(a) The element c in $S(\square)$ has order 4, since the smallest (positive) number of times that we need to apply c to bring the square back to its starting position is 4.

(b) The element r in $S(\square)$ has order 2, since the smallest (positive) number of times that we need to apply r to bring the square back to its starting position is 2.

(c) The smallest positive value of n such that

$$\underbrace{1 +_6 1 +_6 \cdots +_6 1}_{n \text{ copies of } 1} = 0$$

is 6, so 1 in $(\mathbb{Z}_6, +_6)$ has order 6.

(d) The smallest positive value of n such that

$$\underbrace{2 +_6 2 +_6 \cdots +_6 2}_{n \text{ copies of } 2} = 0$$

is 3, so 2 in $(\mathbb{Z}_6, +_6)$ has order 3.

(e) In $(U_9, \times_9)$ we have

$$\begin{aligned} 5^2 &= 5 \times_9 5 = 7, \\ 5^3 &= 5^2 \times_9 5 = 7 \times_9 5 = 8, \\ 5^4 &= 5^3 \times_9 5 = 8 \times_9 5 = 4, \\ 5^5 &= 5^4 \times_9 5 = 4 \times_9 5 = 2, \\ 5^6 &= 5^5 \times_9 5 = 2 \times_9 5 = 1. \end{aligned}$$

So the element 5 in $(U_9, \times_9)$ has order 6.

(f) In $(U_{10}, \times_{10})$ we have

$$9^2 = 9 \times_{10} 9 = 1.$$

So the element 9 in $(U_{10}, \times_{10})$ has order 2.

(g) No positive multiple of 1 in $(\mathbb{Z}, +)$ is equal to the identity element 0, so 1 in $(\mathbb{Z}, +)$ has infinite order.

(h) We have

$$\begin{aligned} i^2 &= i \times i = -1, \\ i^3 &= i^2 \times i = (-1) \times i = -i, \\ i^4 &= i^3 \times i = (-i) \times i = 1. \end{aligned}$$

So the element i in $(\mathbb{C}^*, \times)$ has order 4.

Solution to Exercise B53

The identity element 0 of $(\mathbb{Z}, +)$ has order 1, because $1 \times 0 = 0$ and so the smallest positive integer n such that $n0 = 0$ is 1.

All other elements of $(\mathbb{Z}, +)$ have infinite order, because there is no positive multiple of such an element that is equal to 0.

Solution to Exercise B54

Let x be an element of infinite order in the group $(G, \circ)$. We will prove by contradiction that all the powers

$$\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots$$

of x are distinct. Suppose that these powers are *not* distinct. Then

$$x^s = x^t,$$

for some integers s and t with $s < t$. Composing each side of this equation on the right with $(x^s)^{-1}$ gives

$$x^s \circ (x^s)^{-1} = x^t \circ (x^s)^{-1}.$$

Simplifying (using the index laws on the right-hand side) gives

$$e = x^{t-s}.$$

Now $t - s > 0$, so there is a positive power of x that is equal to e. This is a contradiction, since x has infinite order. Thus all the powers of x in the list above are distinct.

Solution to Exercise B55

(a) The identity element e of $S(\triangle)$ has order 1.

For the element a, we have

$$\begin{aligned} a^2 &= a \circ a = b, \\ a^3 &= a^2 \circ a = b \circ a = e. \end{aligned}$$

Thus a has order 3. Hence b, the inverse of a, also has order 3.

All the other elements of $S(\triangle)$ are self-inverse and hence have order 2.

In summary, the orders of the elements of $S(\triangle)$ are as follows.

Element	e	a	b	r	s	t
Order	1	3	3	2	2	2

(b) The identity element e of $S(\square)$ has order 1, and the remaining elements a, r and s are all self-inverse and hence all have order 2. In summary, the orders of the elements are as follows.

Element	e	a	r	s
Order	1	2	2	2

(c) The Cayley table for $(\mathbb{Z}_5^*, \times_5)$ is as follows.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The identity element 1 has order 1.

For the element 2, we have

$$2^2 = 2 \times_5 2 = 4,$$
$$2^3 = 2^2 \times_5 2 = 4 \times_5 2 = 3,$$
$$2^4 = 2^3 \times_5 2 = 3 \times_5 2 = 1.$$

Thus 2 has order 4. Hence 3, the inverse of 2, also has order 4.

The element 4 is self-inverse, so it has order 2.

In summary, the orders of the elements of $(\mathbb{Z}_5^*, \times_5)$ are as follows.

Element	1	2	3	4
Order	1	4	4	2

(d) The identity element 0 of $(\mathbb{Z}_8, +_8)$ has order 1.

For the element 1, we have

$$1 +_8 1 = 2$$
$$1 +_8 1 +_8 1 = 3$$
$$1 +_8 1 +_8 1 +_8 1 = 4$$
$$\vdots$$
$$\underbrace{1 +_8 1 +_8 \cdots +_8 1}_{7 \text{ copies of } 1} = 7$$
$$\underbrace{1 +_8 1 +_8 \cdots +_8 1}_{8 \text{ copies of } 1} = 0$$

Thus 1 has order 8. Hence 7, the inverse of 1, also has order 8.

For the element 2, we have

$$2 +_8 2 = 4$$
$$2 +_8 2 +_8 2 = 6$$
$$2 +_8 2 +_8 2 +_8 2 = 0$$

Thus 2 has order 4. Hence 6, the inverse of 2, also has order 4.

For the element 3, we have

$$3 +_8 3 = 6$$
$$3 +_8 3 +_8 3 = 1$$
$$3 +_8 3 +_8 3 +_8 3 = 4$$
$$3 +_8 3 +_8 3 +_8 3 +_8 3 = 7$$
$$3 +_8 3 +_8 3 +_8 3 +_8 3 +_8 3 = 2$$
$$\underbrace{3 +_8 3 +_8 \cdots +_8 3}_{7 \text{ copies of } 3} = 5$$
$$\underbrace{3 +_8 3 +_8 \cdots +_8 3}_{8 \text{ copies of } 3} = 0$$

Thus 3 has order 8. Hence 5, the inverse of 3, also has order 8.

Finally, for the element 4, we have

$$4 +_8 4 = 0$$

Thus 4 has order 2.

In summary, the orders of the elements of $(\mathbb{Z}_8, +_8)$ are as follows.

Element	0	1	2	3	4	5	6	7
Order	1	8	4	8	2	8	4	8

Solution to Exercise B56

(a) We have $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. (Recall that U_{20} is the set of all integers in $\mathbb{Z}_{20}$ that are coprime to 20.)

The order of the identity element 1 is 1.

The powers of 3 are

$$\ldots, 1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, \ldots.$$

So 3 has order 4.

The element immediately before the identity element 1 in the cycle of powers of 3 is 7, so 7 is the inverse of 3 and hence it also has order 4. Also, the cycle shows that the powers of $9 = 3^2$ are

$$\ldots, 1, 9, 1, 9, 1, 9, \ldots,$$

so 9 has order 2.

The powers of 11 are

$$\ldots, 1, 11, 1, 11, 1, 11, \ldots,$$

so 11 has order 2.

The powers of 13 are

$$\ldots, 1, 13, 9, 17, 1, 13, 9, 17, 1, 13, 9, 17, \ldots.$$

So 13 has order 4, and 17 is the inverse of 13 and also has order 4.

Finally, the powers of 19 are

$$\ldots, 1, 19, 1, 19, 1, 19, \ldots,$$

so 19 has order 2.

In summary, the orders of the elements of $(U_{20}, \times_{20})$ are as follows.

Element	1	3	7	9	11	13	17	19
Order	1	4	4	2	2	4	4	2

(b) We have $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

The order of the identity element 0 is 1.

The multiples of 1 are

$$\ldots, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0, 1, 2, 3, \ldots.$$

So 1 has order 12. Hence 11, the inverse of 1, also has order 12.

The multiples of 2 are

$$\ldots, 0, 2, 4, 6, 8, 10, 0, 2, 4, 6, 8, 10, \ldots.$$

So 2 has order 6, and 10, the inverse of 2, also has order 6.

The multiples of 3 are

$$\ldots, 0, 3, 6, 9, 0, 3, 6, 9, \ldots.$$

So 3 has order 4, and 9, the inverse of 3, also has order 4.

The multiples of 4 are

$$\ldots, 0, 4, 8, 0, 4, 8, \ldots.$$

So 4 has order 3, and 8, the inverse of 4, also has order 3.

The multiples of 5 are

$$\ldots, 0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0, 5, 10, 3, \ldots.$$

So 5 has order 12, and 7, the inverse of 5, also has order 12.

The multiples of 6 are

$$\ldots, 0, 6, 0, 6, 0, 6, \ldots.$$

So 6 has order 2.

In summary, the orders of the elements of $(\mathbb{Z}_{12}, +_{12})$ are as follows.

Element	0	1	2	3	4	5	6	7	8	9	10	11
Order	1	12	6	4	3	12	2	12	3	4	6	12

Solution to Exercise B57

(a) In $S(\triangle)$, the powers of a repeatedly cycle through the values e, a, b, so

$$\langle a \rangle = \{e, a, b\}.$$

(b) In $(\mathbb{Z}_7^*, \times_7)$, we have

$$\begin{aligned}
3^1 &= 3,\\
3^2 &= 3 \times_7 3 = 2,\\
3^3 &= 3^2 \times_7 3 = 2 \times_7 3 = 6,\\
3^4 &= 3^3 \times_7 3 = 6 \times_7 3 = 4,\\
3^5 &= 3^4 \times_7 3 = 4 \times_7 3 = 5,\\
3^6 &= 3^5 \times_7 3 = 5 \times_7 3 = 1,
\end{aligned}$$

so

$$\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\} = \mathbb{Z}_7^*.$$

(So the subset of $\mathbb{Z}_7^*$ generated by 3 is the whole of $\mathbb{Z}_7^*$. We will look in more detail at groups and group elements for which this happens later in this section.)

(c) In $(\mathbb{Z}, +)$, we have

$$\begin{aligned}
\langle 2 \rangle &= \{2k : k \in \mathbb{Z}\}\\
&= \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}.
\end{aligned}$$

Solution to Exercise B58

We can use the cycles of powers/multiples, and self-inverse elements, found in the solution to Exercise B55. We can cut down the working by using the fact that an element and its inverse generate the same cyclic subgroup.

(a) In $S(\triangle)$ we have

$$\langle e\rangle = \{e\},$$
$$\langle a\rangle = \{e, a, b\},$$
$$\langle b\rangle = \{e, a, b\},$$
$$\langle r\rangle = \{e, r\},$$
$$\langle s\rangle = \{e, s\},$$
$$\langle t\rangle = \{e, t\}.$$

(b) In $S(\square)$ we have

$$\langle e\rangle = \{e\},$$
$$\langle a\rangle = \{e, a\},$$
$$\langle r\rangle = \{e, r\},$$
$$\langle s\rangle = \{e, s\}.$$

(c) In $(\mathbb{Z}_5^*, \times_5)$ we have

$$\langle 1\rangle = \{1\},$$
$$\langle 2\rangle = \{1, 2, 3, 4\} = \mathbb{Z}_5^*,$$
$$\langle 3\rangle = \{1, 2, 3, 4\} = \mathbb{Z}_5^*,$$
$$\langle 4\rangle = \{1, 4\}.$$

(d) In $(\mathbb{Z}_8, +_8)$ we have

$$\langle 0\rangle = \{0\},$$
$$\langle 1\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8,$$
$$\langle 2\rangle = \{0, 2, 4, 6\},$$
$$\langle 3\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8,$$
$$\langle 4\rangle = \{0, 4\},$$
$$\langle 5\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8,$$
$$\langle 6\rangle = \{0, 2, 4, 6\},$$
$$\langle 7\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8.$$

Solution to Exercise B59

(a) $r_{\pi/4}$ has order 8, since its powers $r_{\pi/4},\ r_{\pi/4}^2,\ \ldots,\ r_{\pi/4}^8$ in order are

$$r_{\pi/4},\ r_{\pi/2},\ r_{3\pi/4},\ r_{\pi},\ r_{5\pi/4},\ r_{3\pi/2},\ r_{7\pi/4},\ r_0.$$

(Remember that $r_{2\pi} = r_0$, and that r_0 is the identity element.)

Hence $\langle r_{\pi/4}\rangle$ has order 8.

(b) $r_{\pi/3}$ has order 6, since its powers $r_{\pi/3},\ r_{\pi/3}^2,\ \ldots,\ r_{\pi/3}^6$ in order are

$$r_{\pi/3},\ r_{2\pi/3},\ r_{\pi},\ r_{4\pi/3},\ r_{5\pi/3},\ r_0.$$

Hence $\langle r_{\pi/3}\rangle$ has order 6.

(c) $r_{2\pi/7}$ has order 7, since its powers $r_{2\pi/7},\ r_{2\pi/7}^2,\ \ldots,\ r_{2\pi/7}^7$ in order are

$$r_{2\pi/7},\ r_{4\pi/7},\ r_{6\pi/7},\ r_{8\pi/7},\ r_{10\pi/7},\ r_{12\pi/7},\ r_0.$$

Hence $\langle r_{2\pi/7}\rangle$ has order 7.

(d) r_2 has infinite order. Its powers $r_2,\ r_2^2,\ r_2^3,\ \ldots$ in order are

$$r_2,\ r_4,\ r_6,\ r_8,\ \ldots.$$

Since π is irrational, no suffix is a multiple of 2π, so there is no positive integer n such that $r_2^n = r_0$. Hence $\langle r_2\rangle$ has infinite order.

Solution to Exercise B60

We use the orders of the elements, found in Exercise B55.

(a) $S(\triangle)$ is not cyclic, because it has order 6 but does not contain an element of order 6.

(b) $S(\square)$ is not cyclic, because it has order 4 but does not contain an element of order 4.

(c) $(\mathbb{Z}_5^*, \times_5)$ is cyclic. It has order 4 and contains two elements, namely 2 and 3, of order 4.

(d) $(\mathbb{Z}_8, +_8)$ is cyclic. It has order 8 and contains four elements, namely 1, 3, 5 and 7, of order 8.

Solution to Exercise B61

Let a be a generator of $(G, \circ)$. Let $g, h \in G$; then $g = a^j$ and $h = a^k$ for some $j, k \in \mathbb{Z}$. Hence

$$\begin{aligned} g \circ h &= a^j \circ a^k \\ &= a^{j+k} \\ &= a^{k+j} \\ &= a^k \circ a^j \\ &= h \circ g. \end{aligned}$$

This shows that $(G, \circ)$ is abelian.

Solution to Exercise B62

(a) Since $(\mathbb{Z}_5^*, \times_5)$ is cyclic, all its subgroups are cyclic. From Exercise B58(c), for $(\mathbb{Z}_5^*, \times_5)$ we have

$$\langle 1\rangle = \{1\},$$
$$\langle 2\rangle = \{1, 2, 3, 4\} = \mathbb{Z}_5^*,$$
$$\langle 3\rangle = \{1, 2, 3, 4\} = \mathbb{Z}_5^*,$$
$$\langle 4\rangle = \{1, 4\}.$$

So the distinct subgroups of $(\mathbb{Z}_5^*, \times_5)$ are

$$\{1\}, \quad \{1, 4\}, \quad \mathbb{Z}_5^*.$$

(b) Since $(\mathbb{Z}_8, +_8)$ is cyclic, all its subgroups are cyclic. From Exercise B58(d), for $(\mathbb{Z}_8, +_8)$ we have

$$\langle 0\rangle = \{0\},$$
$$\langle 1\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8,$$
$$\langle 2\rangle = \{0, 2, 4, 6\},$$
$$\langle 3\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8,$$
$$\langle 4\rangle = \{0, 4\},$$
$$\langle 5\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8,$$
$$\langle 6\rangle = \{0, 2, 4, 6\},$$
$$\langle 7\rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8.$$

So the distinct subgroups of $(\mathbb{Z}_8, +_8)$ are

$$\{0\}, \quad \{0, 4\}, \quad \{0, 2, 4, 6\}, \quad \mathbb{Z}_8.$$

Solution to Exercise B63

The generators of $(\mathbb{Z}_8, +_8)$ are 1, 3, 5 and 7.

Solution to Exercise B64

(a) $U_{18} = \{1, 5, 7, 11, 13, 17\}$.

(b) We find the cyclic subgroup generated by each element of $(U_{18}, \times_{18})$:

$$\langle 1\rangle = \{1\},$$
$$\langle 5\rangle = \{1, 5, 7, 17, 13, 11\} = U_{18} = \langle 5^{-1}\rangle = \langle 11\rangle,$$
$$\langle 7\rangle = \{1, 7, 13\} = \langle 7^{-1}\rangle = \langle 13\rangle,$$
$$\langle 17\rangle = \{1, 17\}.$$

(c) Since the element 5, for example, of $(U_{18}, \times_{18})$ generates the whole group, $(U_{18}, \times_{18})$ is cyclic.

Its generators are 5 and 11.

Solution to Exercise B65

We have

$$U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\},$$

so $(U_{20}, \times_{20})$ has order 8.

However, the solution to Exercise B56(a) shows that $(U_{20}, \times_{20})$ does not contain an element of order 8. Therefore $(U_{20}, \times_{20})$ is not cyclic.

Solution to Exercise B66

By the solution to Exercise B64, the group $(U_{18}, \times_{18})$ is cyclic, so all its subgroups are cyclic. Hence its subgroups are those found in the solution to Exercise B64:

$$\{1\}, \quad \{1, 17\}, \quad \{1, 7, 13\}, \quad U_{18}.$$

Solution to Exercise B67

The Cayley table for $(\{1, 9, 11, 19\}, \times_{20})$ is as follows.

$\times_{20}$	1	9	11	19
1	1	9	11	19
9	9	1	19	11
11	11	19	1	9
19	19	11	9	1

We show that the three subgroup properties hold.

SG1 All the elements in the body of the table are in $\{1, 9, 11, 19\}$, so $\{1, 9, 11, 19\}$ is closed under $\times_{20}$.

SG2 The identity element of $(U_{20}, \times_{20})$ is 1, and $1 \in \{1, 9, 11, 19\}$.

SG3 Each element in $\{1, 9, 11, 19\}$ is self-inverse, so $\{1, 9, 11, 19\}$ contains the inverse of each of its elements.

Hence $(\{1, 9, 11, 19\}, \times_{20})$ satisfies the three subgroup properties, and so is a subgroup.

Finally, $(\{1, 9, 11, 19\}, \times_{20})$ is not cyclic: each element is self-inverse, so no element generates the whole subgroup {1, 9, 11, 19}.

Solution to Exercise B68

The identity element 0 has order 1.

The multiples of 1 in $(\mathbb{Z}_5, +_5)$ are

$$\ldots, 0, 1, 2, 3, 4, 0, \ldots.$$

So 1 has order 5, and 4, the inverse of 1, also has order 5.

The multiples of 2 in $(\mathbb{Z}_5, +_5)$ are

$$\ldots, 0, 2, 4, 1, 3, 0, \ldots.$$

So 2 has order 5, and 3, the inverse of 2, also has order 5.

In summary, the orders of the elements of $(\mathbb{Z}_5, +_5)$ are as follows.

Element	0	1	2	3	4
Order	1	5	5	5	5

Solution to Exercise B69

(a) The order of the identity element 0 in $(\mathbb{Z}_6, +_6)$ is 1.

The HCF of 1 and 6 is 1, so the order of 1 is $6/1 = 6$.

The HCF of 2 and 6 is 2, so the order of 2 is $6/2 = 3$.

The HCF of 3 and 6 is 3, so the order of 3 is $6/3 = 2$.

The HCF of 4 and 6 is 2, so the order of 4 is $6/2 = 3$.

The HCF of 5 and 6 is 1, so the order of 5 is $6/1 = 6$.

In summary, the orders of the elements of $(\mathbb{Z}_6, +_6)$ are as follows.

Element	0	1	2	3	4	5
Order	1	6	3	2	3	6

This agrees with the values in the table at the start of this subsection.

(b) The order of the identity element 0 in $(\mathbb{Z}_5, +_5)$ is 1.

All other elements are coprime to 5 and hence the HCF of each of these elements and 5 is 1. Hence all other elements have order 5.

In summary, the orders of the elements of $(\mathbb{Z}_5, +_5)$ are as follows.

Element	0	1	2	3	4
Order	1	5	5	5	5

This agrees with the solution to Exercise B68.

Solution to Exercise B70

(a) The generators of $(\mathbb{Z}_7, +_7)$ are 1, 2, 3, 4, 5 and 6 (all the non-zero elements of $\mathbb{Z}_7$).

(b) The generators of $(\mathbb{Z}_{10}, +_{10})$ are 1, 3, 7 and 9.

Solution to Exercise B71

(a) By Theorem B41, $(\mathbb{Z}_{12}, +_{12})$ has six subgroups, with orders 1, 2, 3, 4, 6 and 12 (the factors of 12):

$$\begin{aligned}
\langle 0 \rangle &= \{0\},\\
\langle 6 \rangle &= \{0, 6\},\\
\langle 4 \rangle &= \{0, 4, 8\},\\
\langle 3 \rangle &= \{0, 3, 6, 9\},\\
\langle 2 \rangle &= \{0, 2, 4, 6, 8, 10\},\\
\langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \mathbb{Z}_{12}.
\end{aligned}$$

(b) By Theorem B41, $(\mathbb{Z}_9, +_9)$ has three subgroups, with orders 1, 3 and 9 (the factors of 9):

$$\begin{aligned}
\langle 0 \rangle &= \{0\},\\
\langle 3 \rangle &= \{0, 3, 6\},\\
\langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = \mathbb{Z}_9.
\end{aligned}$$

(c) By Theorem B41, $(\mathbb{Z}_{11}, +_{11})$ has two subgroups, with orders 1 and 11 (the factors of 11):

$$\begin{aligned}
\langle 0 \rangle &= \{0\},\\
\langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = \mathbb{Z}_{11}.
\end{aligned}$$

Solution to Exercise B72

(a) A suitable matching is

$$\begin{array}{cccc} e & a & b & c \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 4 & 3 \end{array}.$$

(b) A suitable matching is

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 4 & 3 \end{array}$$

(where the elements of $(\mathbb{Z}_4, +_4)$ are on the top row and the elements of $(\mathbb{Z}_5^*, \times_5)$ are on the bottom row).

Solution to Exercise B73

(a) The Cayley table of $(U_{12}, \times_{12})$ is as follows.

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

It has the same pattern as the Cayley table of $(S(\square), \circ)$ (in particular, all four of its elements are self-inverse). So $(U_{12}, \times_{12})$ has the same structure as $(S(\square), \circ)$.

(b) The Cayley table of $(U_{10}, \times_{10})$ is as follows.

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Swapping 7 and 9 in the borders of the table gives the following table.

$\times_{10}$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

It has the same pattern as the Cayley table of $(\mathbb{Z}_4, +_4)$ (in particular, it has exactly two self-inverse elements). So $(U_{10}, \times_{10})$ has the same structure as $(\mathbb{Z}_4, +_4)$.

Solution to Exercise B74

(a) An isomorphism is

$$\begin{aligned} \phi : S(\square) &\longrightarrow U_{12} \\ e &\longmapsto 1 \\ a &\longmapsto 5 \\ r &\longmapsto 7 \\ s &\longmapsto 11. \end{aligned}$$

(There are other possibilities; in fact any one-to-one and onto mapping ϕ that maps e to 1 will do.)

(b) An isomorphism is

$$\begin{aligned} \phi : \mathbb{Z}_4 &\longrightarrow U_{10} \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 3 \\ 2 &\longmapsto 9 \\ 3 &\longmapsto 7. \end{aligned}$$

(There is one other possibility, namely

$$\begin{aligned} \phi : \mathbb{Z}_4 &\longrightarrow U_{10} \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 7 \\ 2 &\longmapsto 9 \\ 3 &\longmapsto 3.) \end{aligned}$$

Solution to Exercise B75

We must show that ϕ is one-to-one and onto, and that for all $m, n \in \mathbb{Z}$,

$$\phi(m+n) = \phi(m) + \phi(n).$$

To check that ϕ is one-to-one, let $m, n \in \mathbb{Z}$ and suppose that $\phi(m) = \phi(n)$; that is,

$$6m = 6n.$$

Then $m = n$. Thus ϕ is one-to-one.

Also, ϕ is onto because each element $6n \in 6\mathbb{Z}$ is the image under ϕ of the element $n \in \mathbb{Z}$.

Finally, for all $m, n \in \mathbb{Z}$,

$$\phi(m+n) = 6(m+n) = 6m + 6n = \phi(m) + \phi(n).$$

Hence ϕ is an isomorphism, so $(\mathbb{Z}, +) \cong (6\mathbb{Z}, +)$.

Solution to Exercise B76

We have $U_{12} = \{1, 5, 7, 11\}$, so $(U_{12}, \times_{12})$ is a group of order 4. Also,

$$\begin{aligned} 1 \times_{12} 1 &= 1, \\ 5 \times_{12} 5 &= 1, \\ 7 \times_{12} 7 &= 1, \\ 11 \times_{12} 11 &= 1, \end{aligned}$$

so all four elements of $(U_{12}, \times_{12})$ are self-inverse. Hence $(U_{12}, \times_{12})$ is isomorphic to the Klein four-group V.

The group $(S(\square), \circ)$ also has order 4 and all four of its elements are self-inverse (since its elements are the identity, two reflections and the rotation through π). Hence it is also isomorphic to V.

Since both groups are isomorphic to V, they are isomorphic to each other.

Solution to Exercise B77

We have

$$\begin{aligned}\phi(g^3) &= \phi(g^2 \circ g)\\ &= \phi(g^2) * \phi(g)\\ &\qquad \text{(since } \phi \text{ is an isomorphism)}\\ &= (\phi(g))^2 * \phi(g) \quad \text{(by equation (6))}\\ &= \phi(g)^3.\end{aligned}$$

Solution to Exercise B78

(a) $(\mathbb{Z}_8, +_8)$ has order 8 and $(S(\triangle), \circ)$ has order 6, so these groups are not isomorphic.

(b) The two groups both have order 8, since $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. However, $(\mathbb{Z}_8 +_8)$ is cyclic, but $(U_{20}, \times_{20})$ is not, as determined in the solution to Exercise B65. Hence these groups are not isomorphic.

Solution to Exercise B79

(a) We have

$$U_9 = \{1, 2, 4, 5, 7, 8\}.$$

The cyclic subgroups of $(U_9, \times_9)$ are

$$\begin{aligned}\langle 1\rangle &= \{1\},\\ \langle 2\rangle &= \{1, 2, 4, 8, 7, 5\},\\ \langle 4\rangle &= \{1, 4, 7\},\\ \langle 5\rangle &= \{1, 5, 7, 8, 4, 2\},\\ \langle 7\rangle &= \{1, 7, 4\},\\ \langle 8\rangle &= \{1, 8\}.\end{aligned}$$

Thus $(U_9, \times_9)$ is cyclic, and its generators are 2 and 5.

(It is not necessary to calculate the elements of $\langle 5\rangle$ and $\langle 7\rangle$, because

$$\langle 2\rangle = \langle 2^{-1}\rangle = \langle 5\rangle \quad \text{and} \quad \langle 4\rangle = \langle 4^{-1}\rangle = \langle 7\rangle.$$

However, you may prefer to use this as a check, rather than as a shortcut.)

(b) The group $(\mathbb{Z}_6, +_6)$ is generated by 1.

Following Strategy B6, that is, mapping a generator to a generator, we obtain two possible isomorphisms:

$$\begin{array}{ll}\phi_1 : U_9 \longrightarrow \mathbb{Z}_6 & \phi_2 : U_9 \longrightarrow \mathbb{Z}_6\\ 2^0 = 1 \longmapsto 0 \times 1 = 0 & 5^0 = 1 \longmapsto 0 \times 1 = 0\\ 2^1 = 2 \longmapsto 1 \times 1 = 1 & 5^1 = 5 \longmapsto 1 \times 1 = 1\\ 2^2 = 4 \longmapsto 2 \times 1 = 2 & 5^2 = 7 \longmapsto 2 \times 1 = 2\\ 2^3 = 8 \longmapsto 3 \times 1 = 3 & 5^3 = 8 \longmapsto 3 \times 1 = 3\\ 2^4 = 7 \longmapsto 4 \times 1 = 4 & 5^4 = 4 \longmapsto 4 \times 1 = 4\\ 2^5 = 5 \longmapsto 5 \times 1 = 5 & 5^5 = 2 \longmapsto 5 \times 1 = 5.\end{array}$$

We can write these more simply as

$$\begin{array}{ll}\phi_1 : U_9 \longrightarrow \mathbb{Z}_6 & \phi_2 : U_9 \longrightarrow \mathbb{Z}_6\\ 1 \longmapsto 0 & 1 \longmapsto 0\\ 2 \longmapsto 1 & 2 \longmapsto 5\\ 4 \longmapsto 2 & 4 \longmapsto 4\\ 5 \longmapsto 5 & 5 \longmapsto 1\\ 7 \longmapsto 4 & 7 \longmapsto 2\\ 8 \longmapsto 3, & 8 \longmapsto 3.\end{array}$$

(Note that although there is one other generator of $(\mathbb{Z}_6, +_6)$, namely 5, mapping the generators 2 and 5 of $(U_9, \times_9)$ in turn to 5 results in the same isomorphisms ϕ_1 and ϕ_2 as above. So ϕ_1 and ϕ_2 are the only isomorphisms from $(U_9, \times_9)$ to $(\mathbb{Z}_6, +_6)$.)

Solution to Exercise B80

(a) The cyclic subgroups of $(U_{17}, \times_{17})$ generated by the elements of G are

$$\begin{aligned}\langle 1\rangle &= \{1\},\\ \langle 2\rangle &= \{1, 2, 4, 8, 16, 15, 13, 9\} = \langle 2^{-1}\rangle = \langle 9\rangle,\\ \langle 4\rangle &= \{1, 4, 16, 13\} = \langle 4^{-1}\rangle = \langle 13\rangle,\\ \langle 8\rangle &= \{1, 8, 13, 2, 16, 9, 4, 15\} = \langle 8^{-1}\rangle = \langle 15\rangle,\\ \langle 16\rangle &= \{1, 16\}.\end{aligned}$$

Thus

$$G = \langle 2\rangle = \langle 9\rangle = \langle 8\rangle = \langle 15\rangle,$$

and it follows that G is a cyclic group under $\times_{17}$, with generators 2, 8, 9 and 15.

(b) The group C is generated by x.

Following Strategy B6, that is, mapping a generator to a generator, we obtain the four isomorphisms $\phi : G \longrightarrow C$ given below. These correspond to

$$2 \longmapsto x, \quad 8 \longmapsto x, \quad 9 \longmapsto x \quad \text{and} \quad 15 \longmapsto x,$$

respectively.

$1 \longmapsto e$	$1 \longmapsto e$	$1 \longmapsto e$	$1 \longmapsto e$
$2 \longmapsto x$	$2 \longmapsto x^3$	$2 \longmapsto x^7$	$2 \longmapsto x^5$
$4 \longmapsto x^2$	$4 \longmapsto x^6$	$4 \longmapsto x^6$	$4 \longmapsto x^2$
$8 \longmapsto x^3$	$8 \longmapsto x$	$8 \longmapsto x^5$	$8 \longmapsto x^7$
$9 \longmapsto x^7$	$9 \longmapsto x^5$	$9 \longmapsto x$	$9 \longmapsto x^3$
$13 \longmapsto x^6$	$13 \longmapsto x^2$	$13 \longmapsto x^2$	$13 \longmapsto x^6$
$15 \longmapsto x^5$	$15 \longmapsto x^7$	$15 \longmapsto x^3$	$15 \longmapsto x$
$16 \longmapsto x^4$	$16 \longmapsto x^4$	$16 \longmapsto x^4$	$16 \longmapsto x^4$

(Note that although $(C, \circ)$ is generated by x^3, x^5 and x^7 as well as by x, mapping the generators of $(G, \times_{17})$ in turn to any of these generators of $(C, \circ)$ results in the same four isomorphisms above.)